

EncryptTight User Guide

EncryptTight acts as a transparent overlay that integrates easily into any existing network architecture, providing encryption rules and keys to EncryptTight Enforcement Points.

EncryptTight consists of a suite of tools that performs various tasks of appliance and policy management, including Policy Manager (PM), Key Management System (KMS), and EncryptTight Enforcement Points (ETEPs).



**Customer
Support
Information**

Order toll-free in the U.S.: Call 877-877-BBOX (outside U.S. call 724-746-5500)
FREE technical support 24 hours a day, 7 days a week: Call 724-746-5500 or fax 724-746-0746
Mailing address: Black Box Corporation, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: www.blackbox.com • E-mail: info@blackbox.com

Table of Contents

Preface	13
About This Document	13
Contacting Black Box Technical Support	14
Part I: EncrypTight Installation and Maintenance	
Chapter 1: EncrypTight Overview	17
Distributed Key Topologies	17
EncrypTight Elements	19
EncrypTight Element Management System	20
Policy Manager	20
Key Management System	20
Policy Enforcement Point	21
Point-to-Point Negotiated Topology	22
Security within EncrypTight	23
Secure Communications Between Devices	24
Secure Key Storage within the ETKMS	24
Chapter 2: EncrypTight Deployment Planning	25
EncrypTight Component Connections	25
Management Station Connections	26
ETPM to ETKMS Connections	26
ETPM and ETKMS on the Same Subnetwork	27
ETPM and ETKMS on Different Subnetworks	27
External ETKMS to ETKMS Connections	29
Connections for Backup ETKMSs	29
Connecting Multiple ETKMSs in an IP Network	30
ETKMS to ETKMS Connections in Ethernet Networks	30
ETKMS to PEP Connections	31
ETKMS to PEP Connections in IP Networks	31
ETKMS to PEP Connections in Ethernet Networks	32
Network Clock Synchronization	33
IPv6 Address Support	33
Certificate Support	34
Network Addressing for IP Networks	35
Chapter 3: Installation and Configuration	37
Before You Start	37
Hardware Requirements	38
Software Requirements	38
Firewall Ports	39
EncrypTight Software Installation	39
Installing EncrypTight Software for the First Time	39
Upgrading to a New Version of EncrypTight	40

Uninstalling EncrypTight Software.....	40
Starting EncrypTight.....	40
Exiting EncrypTight.....	41
Management Station Configuration.....	41
Securing the Management Interface.....	42
Enabling the Microsoft FTP Server.....	42
Configuring the Syslog Server.....	43
Installing ETKMSs.....	43
Configuring ETKMSs.....	43
Basic Configuration for Local ETKMSs.....	44
About Local ETKMSs.....	44
Adding a Local ETKMS.....	44
Launching and Stopping a Local ETKMS.....	45
Starting the Local ETKMS Automatically.....	45
Configuring External ETKMSs.....	46
Logging Into the ETKMS.....	47
Changing the Admin Password.....	47
Changing the Root Password.....	48
Configure the Network Connection.....	49
Configure Time and Date Properties.....	51
Check the Status of the Hardware Security Module.....	53
Starting and Stopping the ETKMS Service.....	53
Checking the Status of the ETKMS.....	54
Secure the Server with the Front Bezel.....	54
Configuring Syslog Reporting on the ETKMSs.....	54
Policy Enforcement Point Configuration.....	55
Default User Accounts and Passwords.....	56
Managing Licenses.....	56
Installing Licenses.....	57
Upgrading Licenses.....	58
Upgrading the EncrypTight License.....	58
Upgrading ETEP Licenses.....	58
Next Steps.....	58
Chapter 4: Managing EncrypTight Users.....	61
Working with EncrypTight User Accounts.....	61
Configuring EncrypTight User Authentication.....	62
Managing EncrypTight Accounts.....	65
Changing an EncrypTight User Password.....	66
How EncrypTight Users Work with ETEP Users.....	67
Chapter 5: Maintenance Tasks.....	69
Working with the EncrypTight Workspace.....	69
About the EncrypTight Workspace.....	69
Saving a Workspace to a New Location.....	70
Loading an Existing Workspace.....	71
Moving a Workspace to a New PC.....	72
Deleting a Workspace.....	72
Installing Software Updates.....	73
Step 1: Schedule the Upgrade.....	73

Step 2: Prepare ETPM Status and Renew Keys	74
Step 3: Upgrade the EncryptTight Software	74
Step 4: Verify ETKMS Status and Deploy Policies	74
Step 5: Upgrade PEP Software	75
Step 6: Change the PEP Software Version and Check Status	77
Step 7: Return Status Refresh and Key Renewal to Original Settings	78
Upgrading External ETKMSs	78

Part II: Working with Appliances using ETEMS

Chapter 6: Getting Started with ETEMS..... 83

ETEMS Quick Tour	83
Defining Appliance Configurations	83
Pushing Configurations to Appliances	84
Upgrading Appliance Software	85
Comparing Configurations	85
Maintenance and Troubleshooting	86
Policy and Certificate Support	87
Understanding the ETEMS Workbench	87
Toolbars	89
Status Indicators	90
Understanding Roles	91
EncryptTight User Types	91
ETEP Appliance Roles	91
Modifying Communication Preferences	92

Chapter 7: Provisioning Appliances 95

Provisioning Basics	95
Adding a New Appliance	96
Saving an Appliance Configuration	97
Pushing Configurations to Appliances	97
Viewing Appliance Status	98
Comparing Configurations	100
Filtering Appliances Based on Address	101
Rebooting Appliances	102
Appliance User Management	102
ETEP User Roles	102
Configuring the Password Enforcement Policy	103
User Name Conventions	104
Default Password Policy Conventions	104
Strong Password Policy Conventions	104
Cautions for Strong Password Enforcement	105
Managing Appliance Users	106
Adding ETEP Users	106
Modifying ETEP User Credentials	108
Deleting ETEP Users	108
Viewing ETEP Users	109
Working with Default Configurations	110
Customizing the Default Configuration	110
Restoring the ETEMS Default Configurations	111

Provisioning Large Numbers of Appliances	111
Creating a Configuration Template.....	112
Importing Configurations from a CSV File	112
Importing Remote and Local Interface Addresses	114
Changing Configuration Import Preferences	115
Checking the Time on New Appliances.....	116
Shutting Down Appliances	116
Chapter 8: Managing Appliances	117
Editing Configurations	117
Changing the Management IP Address.....	118
Changing the Address on the Appliance.....	118
Changing the Address in ETEMS	119
Changing the Date and Time.....	120
Changing Settings on a Single Appliance	121
Changing Settings on Multiple Appliances	121
Deleting Appliances	122
Connecting Directly to an Appliance	123
Connecting to the Command Line Interface	123
Upgrading Appliance Software.....	123
Canceling an Upgrade.....	127
What to do if an Upgrade is Interrupted.....	127
Checking Upgrade Status.....	127
Restoring the Backup File System	127
Part III: Using ETPM to Create Distributed Key Policies	
Chapter 9: Getting Started with ETPM	131
Opening ETPM.....	131
About the ETPM User Interface	131
EncryptTight Components View	133
Editors	134
Policy View	135
ETPM Status Indicators.....	135
Sorting and Using Drag and Drop	136
ETPM Toolbar	137
ETPM Status Refresh Interval	137
About ETPM Policies	138
IP Policies.....	138
Ethernet Policies.....	138
Policy Generation and Distribution.....	139
Creating a Policy: An Overview.....	141
Chapter 10: Managing Policy Enforcement Points.....	147
Provisioning PEPs.....	147
Adding a New Appliance	147
Adding a New PEP in ETEMS	148
Adding a New PEP Using ETPM	150
Adding Large Numbers of PEPs.....	150
Pushing the Configuration	151

Editing PEPs	151
Editing PEPs From ETEMS	151
Editing Multiple PEPs	152
Editing PEPs From ETPM	152
Changing the IP Address of a PEP	153
Changing the PEP from Layer 3 to Layer 2 Encryption	153
Deleting PEPs	153
Chapter 11: Managing Key Management Systems	155
Adding ETKMSs	156
Editing ETKMSs	157
Deleting ETKMSs	157
Chapter 12: Managing IP Networks	159
Adding Networks	159
Advanced Uses for Networks in Policies	161
Grouping Networks into Supernet	161
Using Non-contiguous Network Masks	162
Editing Networks	164
Deleting Networks	164
Chapter 13: Managing Network Sets	167
Types of Network Sets	168
Adding a Network Set	170
Importing Networks and Network Sets	172
Editing a Network Set	174
Deleting a Network Set	174
Chapter 14: Creating VLAN ID Ranges for Layer 2 Networks	177
Adding a VLAN ID Range	177
Editing a VLAN ID Range	179
Deleting a VLAN ID Range	179
Chapter 15: Creating Distributed Key Policies	181
Policy Concepts	181
Policy Priority	182
Schedule for Renewing Keys and Refreshing Policy Lifetime	182
Policy Types and Encryption Methods	183
Encapsulation	183
Encryption and Authentication Algorithms	184
Key Generation and ETKMSs	185
Addressing Mode	185
Using Encrypt All Policies with Exceptions	185
Policy Size and ETEP Operational Limits	186
Minimizing Policy Size	187
Adding Layer 2 Ethernet Policies	188
Adding Layer 3 IP Policies	191
Adding a Hub and Spoke Policy	191
Adding a Mesh Policy	195

Adding a Multicast Policy.....	199
Adding a Point-to-point Policy	203
Adding Layer 4 Policies.....	206
Policy Deployment	207
Verifying Policy Rules Before Deployment	207
Deploying Policies	208
Setting Deployment Confirmation Preferences	208
Editing a Policy.....	209
Deleting Policies.....	209
Chapter 16: Policy Design Examples.....	211
Basic Layer 2 Point-to-Point Policy Example	211
Layer 2 Ethernet Policy Using VLAN IDs	212
Complex Layer 3 Policy Example	214
Encrypt Traffic Between Regional Centers.....	214
Encrypt Traffic Between Regional Centers and Branches	215
Passing Routing Protocols	218
Part IV: Troubleshooting	
Chapter 17: ETEMS Troubleshooting	223
Possible Problems and Solutions.....	223
Appliance Unreachable	224
Appliance Configuration	225
Pushing Configurations	226
Status Indicators.....	226
Software Upgrades.....	227
Pinging the Management Port.....	227
Retrieving Appliance Log Files.....	228
Viewing Diagnostic Data	230
Viewing Statistics.....	230
Viewing Port and Discard Status.....	232
Exporting SAD and SPD Files	232
CLI Diagnostic Commands.....	233
Working with the Application Log	234
Viewing the Application Log from within EncrypTight.....	234
Sending Application Log Events to a Syslog Server	235
Exporting the Application Log.....	235
Setting Log Filters.....	235
Other Application Log Actions	236
Chapter 18: ETPM and ETKMS Troubleshooting.....	237
Learning About Problems.....	237
Monitoring Status.....	237
Symptoms and Solutions	238
Policy Errors.....	239
Status Errors	240
Renew Key Errors	240
Viewing Log Files	241
ETPM Log Files.....	241

ETKMS Log Files	241
PEP Log Files	242
ETKMS Troubleshooting Tools	242
ETKMS Server Operation	242
Optimizing Time Synchronization	243
Shutting Down or Restarting an External ETKMS	243
Resetting the Admin Password	243
PEP Troubleshooting Tools	243
Statistics	244
Changing the Date and Time	244
ETEP PEP Policy and Key Information	244
Replacing Licensed ETEPs	245
Troubleshooting Policies	245
Checking Traffic and Encryption Statistics	245
Solving Policy Problems	246
Viewing Policies on a PEP	246
Placing PEPs in Bypass Mode	246
Allowing Local Site Exceptions to Distributed Key Policies	247
Expired Policies	247
Cannot Add a Network Set to a Policy	248
Packet Fragments are Discarded in Point-to-Point Port-based Policies	248
Solving Network Connectivity Problems	248
Modifying EncryTight Timing Parameters	249
Certificate Implementation Errors	249
Cannot Communicate with PEP	249
ETKMS Boot Error	250
Invalid Certificate Error	250
Invalid Parameter in Function Call	250

Part V: Reference

Chapter 19: Modifying the ETKMS Properties File	255
About the ETKMS Properties File	255
Hardware Security Module Configuration	256
Digital Certificate Configuration	256
Logging Setup	256
Base Directory for Storing Operational State Data	257
Peer ETKMS and ETPM Communications Timing	257
Policy Refresh Timing	258
PEP Communications Timing	258
Chapter 20: Using Enhanced Security Features	261
About Enhanced Security Features	261
About Strict Authentication	262
Prerequisites	263
Order of Operations	263
Certificate Information	264
Using Certificates in an EncryTight System	265
Changing the Keystore Password	266

Changing the EncrypTight Keystore Password	266
Changing the ETKMS Keystore Password	266
Changing the Keystore Password on a ETKMS	267
Changing the Keystore Password on a ETKMS with an HSM	268
Configuring the Certificate Policies Extension	269
Working with Certificates for EncrypTight and the ETKMSs	272
Generating a Key Pair	272
Requesting a Certificate	273
Importing a CA Certificate	274
Importing a CA Certificate Reply	274
Exporting a Certificate	275
Working with Certificates and an HSM.....	275
Configuring the HSM for Keytool	275
Importing CA Certificates into the HSM.....	276
Generating a Key Pair for use with the HSM.....	276
Generating a Certificate Signing Request for the HSM	277
Importing Signed Certificates into the HSM.....	277
Working with Certificates for the ETEPs	277
Understanding the Certificate Manager Perspective	278
Certificate Manager Workflow	279
Working with External Certificates	279
Obtaining External Certificates.....	279
Installing an External Certificate.....	280
Working with Certificate Requests.....	281
Requesting a Certificate	281
Installing a Signed Certificate.....	283
Viewing a Pending Certificate Request.....	283
Canceling a Pending Certificate Request	284
Setting Certificate Request Preferences	284
Managing Installed Certificates	285
Viewing a Certificate	286
Exporting a Certificate.....	286
Deleting a Certificate.....	287
Validating Certificates	287
Validating Certificates Using CRLs.....	287
Configuring CRL Usage in EncrypTight and the ETKMSs	288
Configuring CRL Usage on ETEPs	288
Handling Revocation Check Failures	289
Validating Certificates Using OCSP	289
Enabling and Disabling Strict Authentication	292
Removing Certificates	293
Using a Common Access Card	294
Configuring User Accounts for Use With Common Access Cards	295
Enabling Common Access Card Authentication.....	295
Handling Common Name Lookup Failures.....	297
Chapter 21: ETEP Configuration	299
Identifying an Appliance	300
Product Family and Software Version	300
Appliance Name	300
Throughput Speed.....	301

Interface Configuration	301
Management Port Addressing	302
IPv4 Addressing	303
IPv6 Addressing	304
Auto-negotiation - All Ports	305
Remote and Local Port Settings	306
Transparent Mode	306
Local and Remote Port IP Addresses	307
Transmitter Enable	308
DHCP Relay IP Address	309
Ignore DF Bit	310
Reassembly Mode	310
Trusted Hosts	311
SNMP Configuration	313
System Information	313
Community Strings	314
Traps	315
SNMPv2 Trap Hosts	316
SNMPv3	316
Generating the Engine ID	318
Retrieving and Exporting Engine IDs	318
Configuring the SNMPv3 Trap Host Users	319
Logging Configuration	321
Log Event Settings	322
Defining Syslog Servers	323
Log File Management	324
Advanced Configuration	325
Path Maximum Transmission Unit	326
Non IP Traffic Handling	327
CLI Inactivity Timer	327
Password Strength Policy	327
XML-RPC Certificate Authentication	328
SSH Access to the ETEP	329
SNTP Client Settings	329
IKE VLAN Tags	329
OCSP Settings	330
Certificate Policy Extensions	330
Features Configuration	330
FIPS Mode	331
Enabling FIPS Mode	331
Disabling FIPS	332
Verifying FIPS Status on the ETEP	332
EncrypTight Settings	333
Encryption Policy Settings	334
Working with Policies	334
Using EncrypTight Distributed Key Policies	335
Creating Layer 2 Point-to-Point Policies	335
Selecting a Role	337
Using Preshared Keys for IKE Authentication	337
Using Group IDs	337
Selecting the Traffic Handling Mode	338
How the ETEP Encrypts and Authenticates Traffic	338

Factory Defaults	339
Interfaces	339
Trusted Hosts	340
SNMP	340
Logging	341
Policy	341
Advanced	341
Features	342
Hard-coded Settings	342
Index.....	343

Preface

About This Document

Purpose

The *EncrypTight User Guide* provides detailed information on how to install, configure, and troubleshoot EncrypTight components: ETEMS, Policy Manager (ETPM), and Key Management System (ETKMS). It also contains information about configuring EncrypTight Enforcement Points (ETEPs) using ETEMS.

Intended Audience

This document is intended for network managers and security administrators who are familiar with setting up and maintaining network equipment. Some knowledge of network security issues and encryption technologies is assumed.

Assumptions

This document assumes that its readers have an understanding of the following:

- EncrypTight encryption appliance features, installation and operation
- Basic principles of network security issues
- Basic principles of encryption technologies and terminology
- Basic principles of TCP/IP networking, including IP addressing, switching and routing
- Personal computer (PC) operation, common PC terminology, use of terminal emulation software and FTP operations
- Basic knowledge of the Linux operating system

Conventions used in this document

Bold	Indicates one of the following: <ul style="list-style-type: none">• a menu item or button• the name of a command or parameter
<i>Italics</i>	Indicates a new term
Monospaced	Indicates machine text, such as terminal output and filenames
Monospaced bold	Indicates a command to be issued by the user

Contacting Black Box Technical Support

Contact our FREE technical support, 24 hours a day, 7 days a week:

Phone 724-746-5500
Fax 724-746-0746
e-mail info@blackbox.com
Web site www.blackbox.com

Part I EncrypTight Installation and Maintenance



1 EncrypTight Overview

EncrypTight™ Policy and Key Manager is an innovative approach to network-wide encryption. EncrypTight acts as a transparent overlay that integrates easily into any existing network architecture, providing encryption rules and keys to EncrypTight encryption appliances.

EncrypTight consists of a suite of tools that perform various tasks of appliance and policy management:

- EncrypTight Element Management System (ETEMS) is the network management component of the EncrypTight software. Use ETEMS to configure and manage your encryption appliances.
- EncrypTight Policy Manager (ETPM) is the policy generation and management tool. Use ETPM to create policies for hub and spoke, mesh, point-to-point, and multicast networks that require common keys to secure traffic between multiple nodes.
- EncrypTight Key Management System (ETKMS) is the key generation and distribution tool that is used with ETPM-generated policies. ETKMS can be run on a local machine for small deployments or on a dedicated server for larger scale networks.
- EncrypTight Enforcement Points (ETEPs) are the encryption appliances that enforce the security policies. EncrypTight appliances are also referred to as PEPs.

The type of policies that you create, and the tools that you use to create them, are dependent on your network topology. EncrypTight supports two types of policies for the following topologies:

- Distributed key policies are appropriate for securing a variety of networks, including mesh, hub and spoke, point-to-point (Layer 3/4 only), and multicast networks.
- Negotiated policies are appropriate in Layer 2 point-to-point networks where keys are negotiated with a peer rather than distributed from a central key server.

This section includes the following topics:

- [Distributed Key Topologies](#)
- [Point-to-Point Negotiated Topology](#)
- [Security within EncrypTight](#)

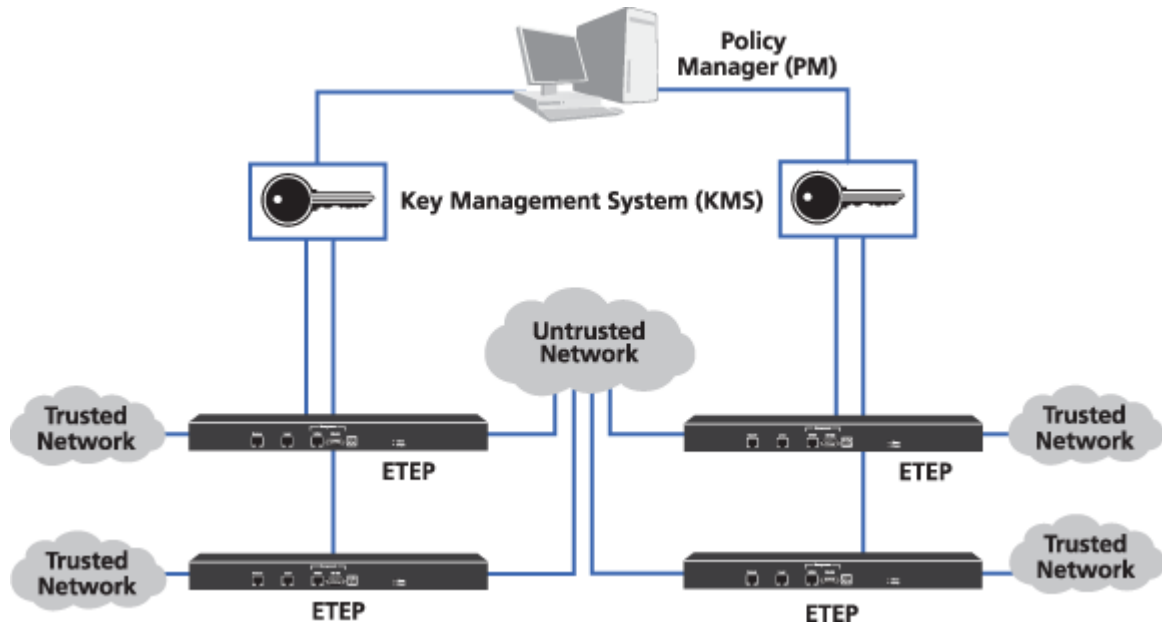
Distributed Key Topologies

EncrypTight centralizes the creation and distribution of encryption keys and policies. It separates the functions of policy management, key generation and distribution, and policy enforcement. By doing so,

multiple Policy Enforcement Points (PEPs) can use common keys, while a centralized platform assumes the function of renewing keys at pre-determined intervals.

In this system, you use ETEMS to configure the PEPs, Policy Manager (ETPM) to create and manage policies, and Key Management System (ETKMS) to generate keys and distribute keys and policies to the appropriate PEPs. The PEPs encrypt traffic according to the policies and keys that they receive.

Figure 1 EncrypTight components



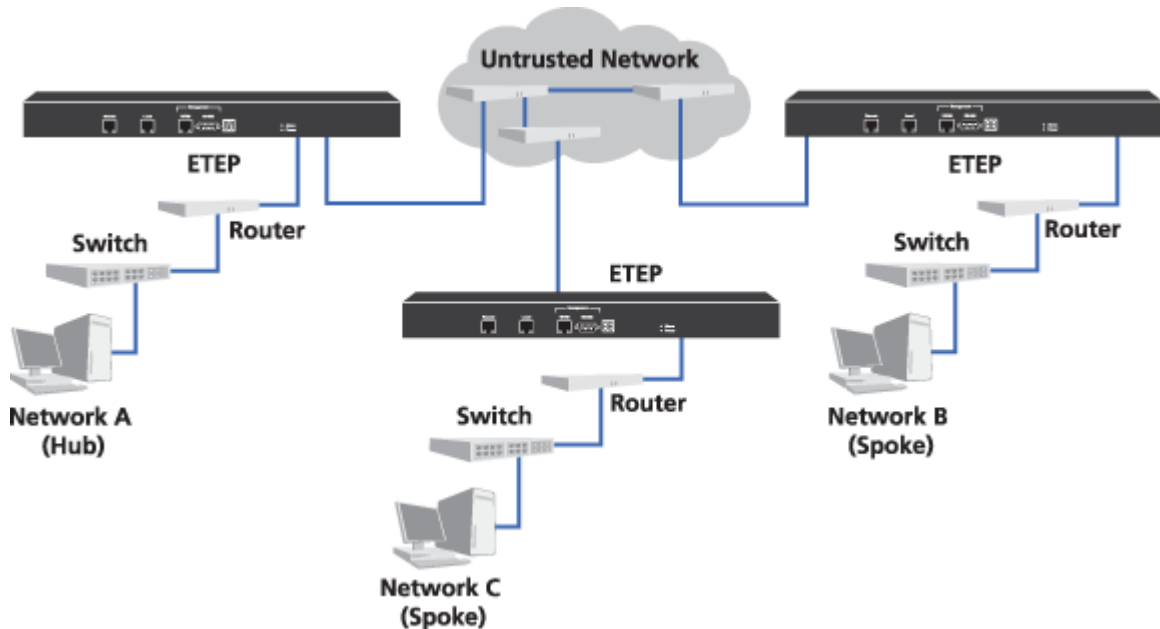
Using EncrypTight, you can create distributed key policies for the network topologies shown in [Table 1](#).

Table 1 Network topologies

Topology	Description
Layer 3 IP topologies	
Hub and Spoke	In a hub and spoke network, a hub network communicates with the spoke networks and the spoke networks communicate only with the hub network.
Multicast	In multicast transmission, one or more networks send unidirectional streams to a multicast network address. The multicast routers detect the multicast transmission, determine which nodes have joined the multicast network as destination networks, and duplicate the packet as needed to reach all multicast destination networks.
Point-to-point	In a point-to-point network, one network sends and receives data to and from one other network.
Mesh	In a mesh network, any network can send or receive data from any other network.
Layer 2 Ethernet topologies	
Mesh	For Ethernet, you can create policies for mesh networks. Note that if the network uses VLAN ID tags, you can also create policies for virtual point-to-point connections.

Regardless of topology, PEPs are typically located at the point in the network where traffic is being sent to an untrusted network or coming from an untrusted network. As an example, [Figure 2](#) shows a hub and spoke network secured with EncrypTight.

Figure 2 PEPs in a Hub and Spoke network



PEP A encrypts data traffic from Network A that goes to Networks B or C. PEP A also decrypts data that originates from Networks B and C. PEP B encrypts data from Network B that goes to Network A and decrypts data that comes from Network A. PEP C encrypts data from Network C that goes to Network A and decrypts data that comes from Network A.

Related topics:

- [“EncrypTight Element Management System”](#) on page 20
- [“Policy Manager”](#) on page 20
- [“Key Management System”](#) on page 20
- [“Policy Enforcement Point”](#) on page 21

EncrypTight Elements

EncrypTight consists of a suite of tools that perform various tasks of appliance and policy management:

- [EncrypTight Element Management System](#) is the element management component of the EncrypTight software
- [Policy Manager](#) is the policy generation and management tool
- [Key Management System](#) is the key generation and distribution tool
- [Policy Enforcement Points](#) are the encryption appliances that enforce the security policies

The number of ETEPs that you can manage and the speed at which they run is controlled by licenses. You must enter a license for EncrypTight before you can install licenses on the ETEPs.

EncrypTight Element Management System

The EncrypTight Element Management System (ETEMS) is the device management component of the EncrypTight software, allowing you to provision and manage multiple encryption appliances from a central location. It provides capabilities for appliance configuration, software updates, and maintenance and troubleshooting for your EncrypTight encryption appliances.

Policy Manager

The Policy Manager (ETPM) is the policy component of the EncrypTight software. You use ETPM to create and manage policies, and monitor the status of the PEPs and ETKMSs.

Each deployment of EncrypTight uses a single ETPM. The ETPM sends metapolicies to one or more ETKMSs. A metapolicy is a file that describes the policies created in ETPM and for each policy it specifies:

- The PEPs each ETKMS controls
- The networks each PEP protects
- The action that is performed (encrypt, send in the clear, or drop)
- The kind of traffic the policy affects

Key Management System

Distribution functions are provided by the EncrypTight Key Management System (ETKMS). All ETKMSs receive policies from a single ETPM. Based on the metapolicies received from the ETPM, the ETKMS generates keys for each of the PEPs within its network. The ETKMS distributes the keys and policies associated with its networks to the appropriate PEPs.

Depending on the size and configuration of your network, you can use a single ETKMS or multiple ETKMSs distributed throughout the network. When multiple ETKMSs are used, each ETKMS controls different sets of PEPs. All ETKMSs include the policy information and keys for the entire network. When policies are deployed or keys are renewed, each PEP receives its information from its designated ETKMS.

The EncrypTight system supports two types of ETKMSs: external ETKMSs and local ETKMSs.

- External ETKMSs are dedicated computers running the ETKMS software. By running on a dedicated computer, external ETKMSs inherently provide more security and reliability, and can be used to help protect significantly larger networks. Each ETKMS can support several hundred PEPs.
- Local ETKMSs run as a separate process on the same management workstation as the EncrypTight software. Local ETKMSs are intended for use with small to medium networks with no more than 10 PEPs. A local ETKMS is included with the EncrypTight software.

[Figure 3](#) shows a single ETKMS distributing the keys for PEPs A, B, C, and D.

Figure 3 Single ETKMS for multiple sites

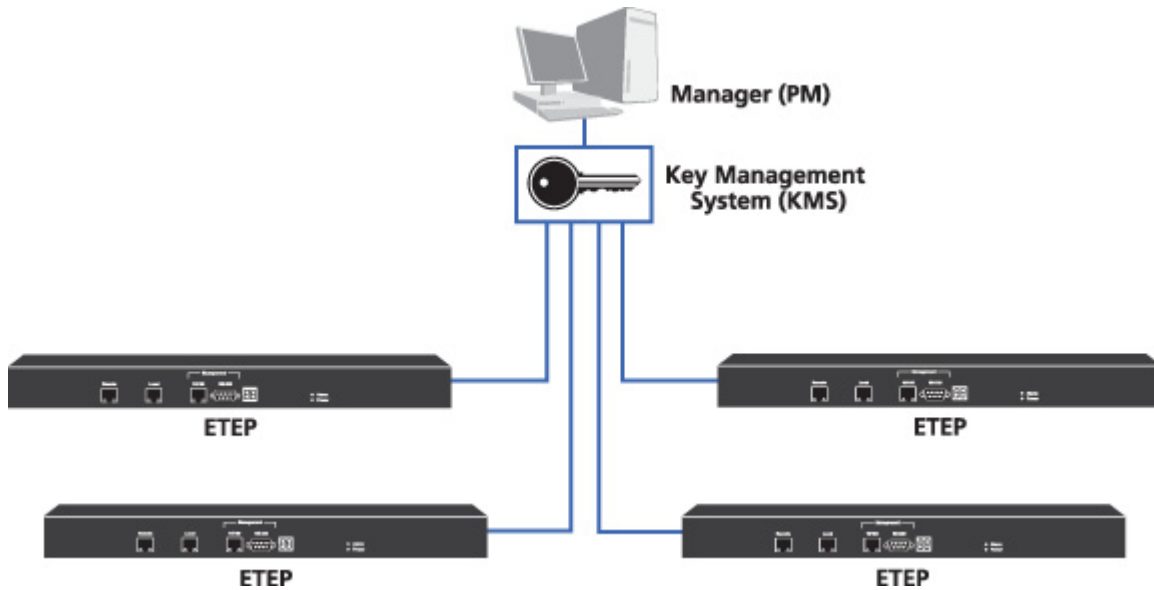
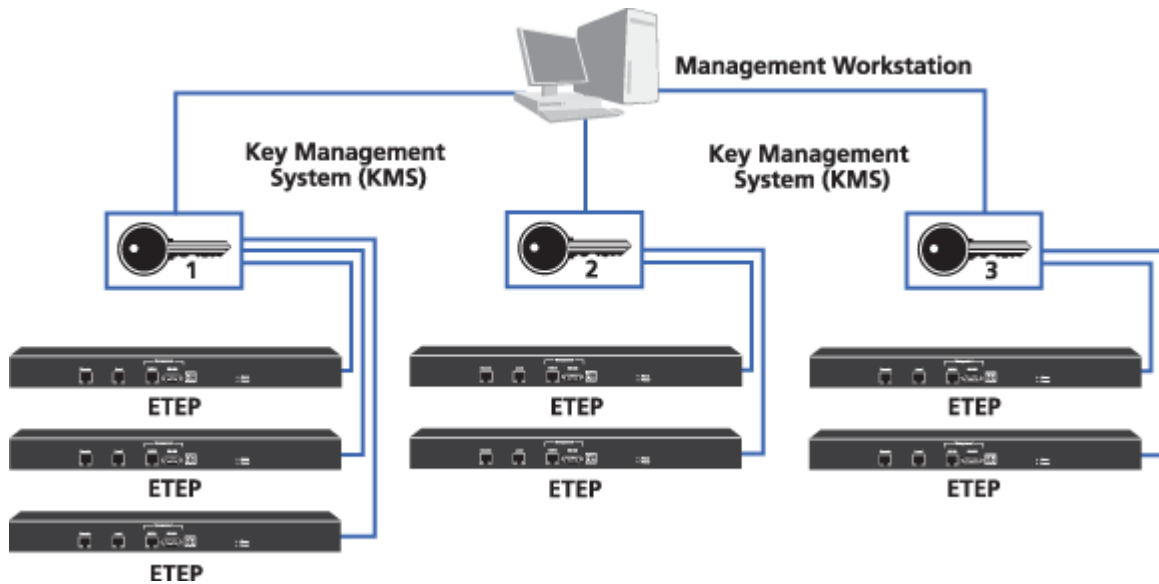


Figure 4 illustrates an EncryptTight deployment using multiple ETKMSs. With large, complex networks that have hundreds of PEPs, you might want to use multiple ETKMSs. Each ETKMS distributes keys for the PEPs it controls. For example: ETKMS 1 distributes the policies and keys to PEPs A, B, and C. ETKMS 2 distributes the policies and keys to PEPs D and E. ETKMS 3 distributes the policies and keys to PEPs F and G.

Figure 4 Multiple ETKMSs in a network

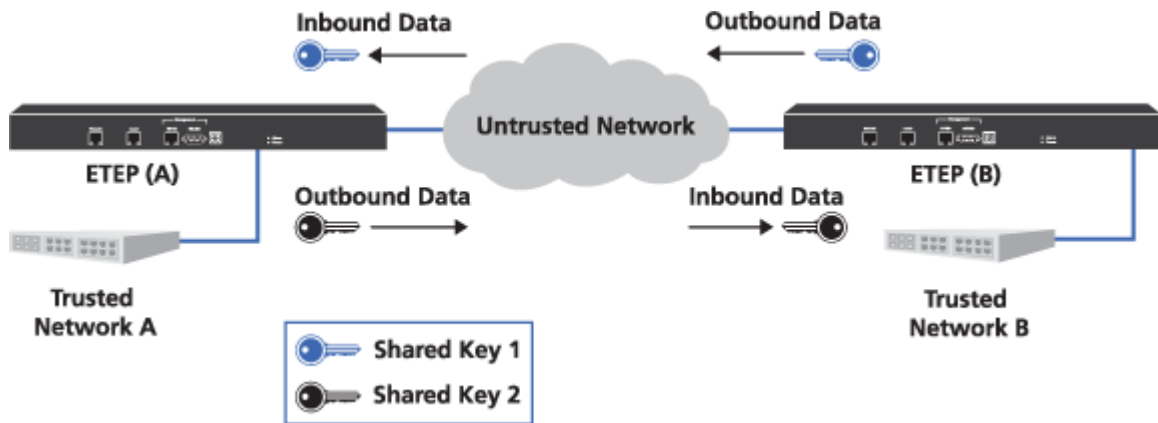


Policy Enforcement Point

EncryptTight enforcement points (ETEPs) are encryption appliances that provide policy enforcement functions, and are referred to generically as PEPs (policy enforcement points). According to the policies distributed by the ETKMSs, the PEPs can encrypt and decrypt traffic, send traffic in the clear, or drop traffic. Each PEP can be used in multiple policies simultaneously.

To securely transfer data between two PEPs over an untrusted network, both PEPs must share a key. One PEP uses the shared key to encrypt the data for transmission over the untrusted network, while the second PEP uses the same shared key to decrypt the data. [Figure 5](#) illustrates the shared key concepts between two PEPs.

Figure 5 Shared keys



In this example, traffic moves between two trusted networks: Network A and Network B. PEP A and PEP B work in unison to insure data security as the traffic passes through an unsecured network. PEP A uses Shared Key 2 to encrypt all outbound traffic intended for Network B. PEP B uses the same shared key to decrypt all traffic inbound from Network A. Traffic flowing in the opposite direction is secured in the same manner using Shared Key 1.

EncryptTight Policy Enforcement Points (PEPs) can be configured for Layer 2 or Layer 3/4 operation. Models include:

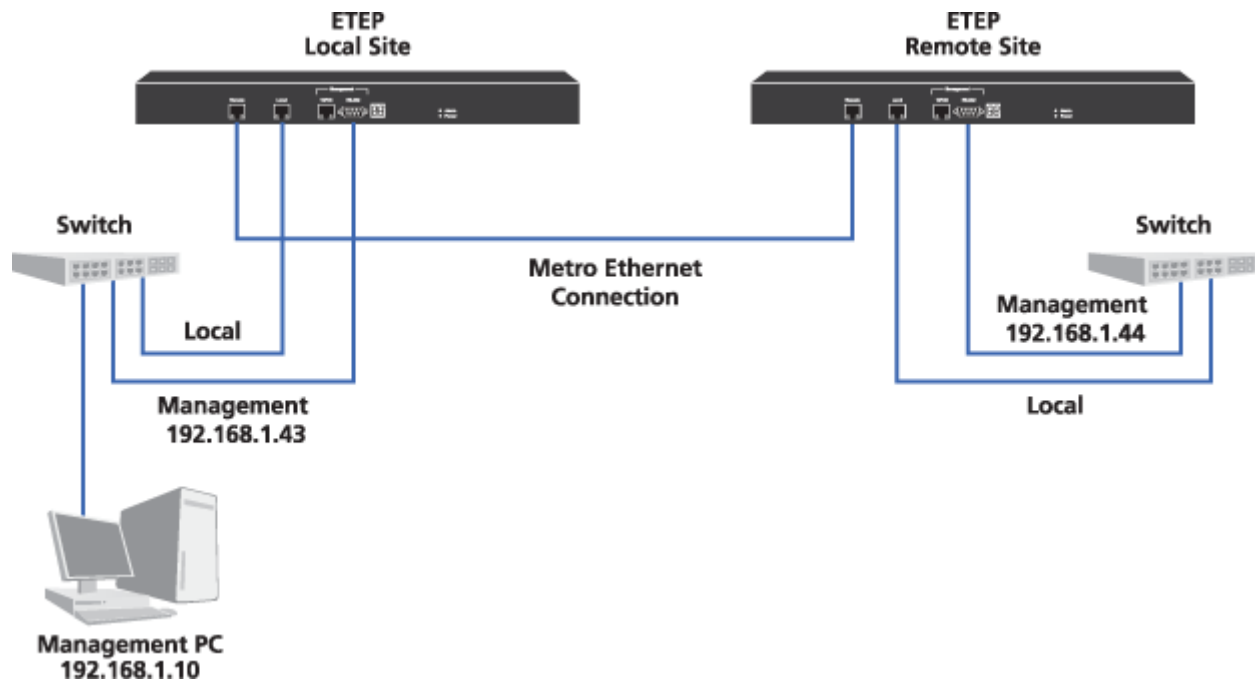
- ET0010A
- ET0010A
- ET1000A

Point-to-Point Negotiated Topology

You can protect simple, point-to-point Ethernet links using ETEMS. Two PEPs can be configured with ETEMS to protect a Layer 2 Ethernet link, without any need for ETPM or ETKMS. The policies and key are negotiated directly by the two PEPs, without requiring a centralized key generation and distribution tool.

This option provides a simple, quick, and straightforward way to secure a single point-to-point Layer 2 Ethernet link. All you need to secure your traffic is ETEMS and two ETEP encryption appliances.

The ETEP can be managed in-line or out-of-band through a dedicated Ethernet management interface, as shown in [Figure 6](#).

Figure 6 Layer 2 Point-to-Point Deployment

Use the Policy Manager (ETPM) and Key Management System (ETKMS) to create a Layer 3 point-to-point distributed key policy as one of several policies in a larger, more complex EncrypTight deployment.

The ETEP's variable speed feature is controlled by the installation of a license. Note that you cannot install a license on the ETEP until you first enter a license for EncrypTight. For more information about licensing, see [“Managing Licenses”](#) on page 56.

Related topics:

- [“Distributed Key Topologies”](#) on page 17
- [“EncrypTight Element Management System”](#) on page 20
- [“Policy Manager”](#) on page 20
- [“Key Management System”](#) on page 20
- [“Policy Enforcement Point”](#) on page 21
- [“Creating Layer 2 Point-to-Point Policies”](#) on page 335

Security within EncrypTight

Because EncrypTight generates keys that provide security throughout a network, it is critical that the EncrypTight components also be secured.

Security in the EncrypTight system has two general areas:

- [“Secure Communications Between Devices”](#) on page 24
- [“Secure Key Storage within the ETKMS”](#) on page 24

Secure Communications Between Devices

Each node in the distributed key system, the EncrypTight management station, the ETKMSs, and the PEPs, communicate policy and status information with other nodes. Given the distributed nature of networks, much of this communication occurs across public networks.

EncrypTight uses Transport Layer Security (TLS) to encrypt management traffic between EncrypTight components. This protocol allows secure communication between the devices in the system while providing information about the secure stream to EncrypTight. You can enhance that security by authenticating the management communications between EncrypTight components using certificates. To learn more about certificates and strict authentication, see [“Using Enhanced Security Features” on page 261](#).

Secure Key Storage within the ETKMS

Key generation and key storage on the ETKMS are critical to maintaining security in EncrypTight. The ETKMS uses the following mechanisms to protect the keys:

- Generates keys using known secure algorithms
- Encrypts keys that are distributed and stored locally
- Limits access to keys to authorized administrators
- Prevents external probing to access or modify keys
- Optionally generates and stores keys in a hardware security module

2 EncrypTight Deployment Planning

When deploying EncrypTight, you must plan the following:

- [EncrypTight Component Connections](#)
- [Network Clock Synchronization](#)
- [IPv6 Address Support](#)
- [Certificate Support](#)
- [Network Addressing for IP Networks](#)

EncrypTight Component Connections

EncrypTight can be managed in-line or out-of-band. When managing in-line, management traffic flows through the data path. You must enable the **Passing TLS traffic in the clear** feature on all PEPs for proper communication among EncrypTight components (ETEMS, ETPM, ETKMS, PEPs). When passing TLS in the clear is enabled on Layer 2 PEPs, TLS and ARP packets are sent unencrypted.

If your network uses other routing protocols that need to pass in the clear, consider the following:

- At Layer 3, create policies to pass the routing protocols in the clear. The PEPs must also be configured to pass non-IP traffic in the clear (this is the default setting on the Advanced tab in ETEMS).
- At Layer 2, consider a separate out-of-band management network, or put the management traffic on a separate VLAN and create a Layer 2 policy to pass packets with this VLAN tag in the clear. Customer support can advise you on a solution that works best in your network.
- Use local site policies

Local site policies allow you to create locally configured policies using CLI commands, without requiring an EncrypTight ETKMS for key distribution. Using the local-site CLI commands you can create manual key encryption policies, bypass policies, and discard policies at either Layer 2 or Layer 3. Mesh policies can be created by adding policies that share the identical keys and SPIs to multiple ETEPs.

The primary use for local site policies is to facilitate in-line management in Layer 2 encrypted networks. These policies supplement existing encryption policies, adding the flexibility to encrypt or pass in the clear specific Layer 3 routing protocols, or Layer 2 Ethertypes and VLAN IDs.

For information on creating and using local site policies, see the *CLI User Guide*.

This chapter discusses connections between each of the EncrypTight components, providing in-line and out-of-band examples.

- [“Management Station Connections” on page 26](#)

The EncrypTight software includes ETEMS for appliance configuration, ETPM for policy management, and a local ETKMS. The local ETKMS deploys keys and policies to all of the PEPs that it manages and checks the PEPs’ status. The management station also uses other services such as NTP, syslog, and SNMP.
- [“ETPM to ETKMS Connections” on page 26](#)

The ETPM passes metapolicies to the ETKMSs and checks the status of the PEPs through the ETKMSs.
- [“External ETKMS to ETKMS Connections” on page 29](#)

When multiple ETKMSs are used in a system, the ETKMSs must be able to share keys. If you set up a ETKMS to serve as a backup for another ETKMS, the backup ETKMS periodically checks the status of the primary ETKMS in case of ETKMS failure.
- [“ETKMS to PEP Connections” on page 31](#)

Each ETKMS deploys keys and policies to all of the PEPs that it manages and checks the PEPs status.

Management Station Connections

Keep the following items in mind when setting up your management connections:

- PEPs can be managed in-line or out-of-band. When managing the PEPs in-line, management traffic flows through the data path. In distributed key deployments, enable the **Pass TLS traffic in the clear** option on the PEPs to ensure proper communication between the PEP and other EncrypTight components. This is configured on the Features tab of the ETEMS Appliance editor.
- The PEP management ports and management services such as NTP, syslog, and SNMP must be directly addressable on the same network.
- EncrypTight to PEP connections when using a local ETKMS:

The EncrypTight software includes ETEMS, ETPM and local ETKMS. When you use a local ETKMS, the ETKMS software runs as a separate process on the same workstation as the ETPM software. In this scenario, ETPM communicates directly with the ETKMS without using a network connection.

The communications between the local ETKMS and the PEPs require a connection between an Ethernet port on the management workstation and the management port on each PEP. For these connections, follow the same general guidelines as external ETKMSs, outlined in [“ETKMS to PEP Connections” on page 31](#). The only difference is that the connections originate from the management workstation and not an external ETKMS.

ETPM to ETKMS Connections

The ETPM sends metapolicies to the ETKMSs and checks the status of the PEPs through the ETKMSs. The communications between EncrypTight components depend on a connection between the Ethernet ports on each device. External ETKMSs can be located on the same subnetwork with the ETPM, or the ETPM and ETKMSs can be located on different subnetworks. If you use a local ETKMS, ETPM communicates directly with the ETKMS without using a network connection.

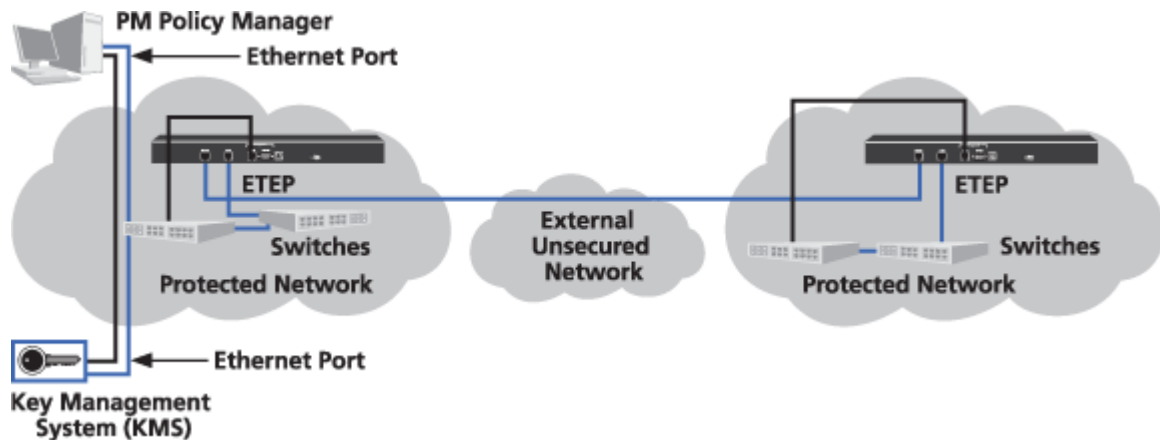
This section describes the planning for the following connections:

- “ETPM and ETKMS on the Same Subnetwork” on page 27
- “ETPM and ETKMS on Different Subnetworks” on page 27

ETPM and ETKMS on the Same Subnetwork

When the ETPM is located on the same subnetwork as the external ETKMS, the ETPM communicates with the ETKMS over the internal protected network using Ethernet connections as shown in [Figure 7](#).

Figure 7 ETPM and ETKMS located in the same subnetwork



ETPM and ETKMS on Different Subnetworks

The ETPM and ETKMS interconnections on different subnetworks depends on the type of policy: Layer 3 IP policy or Layer 2 Ethernet policy.

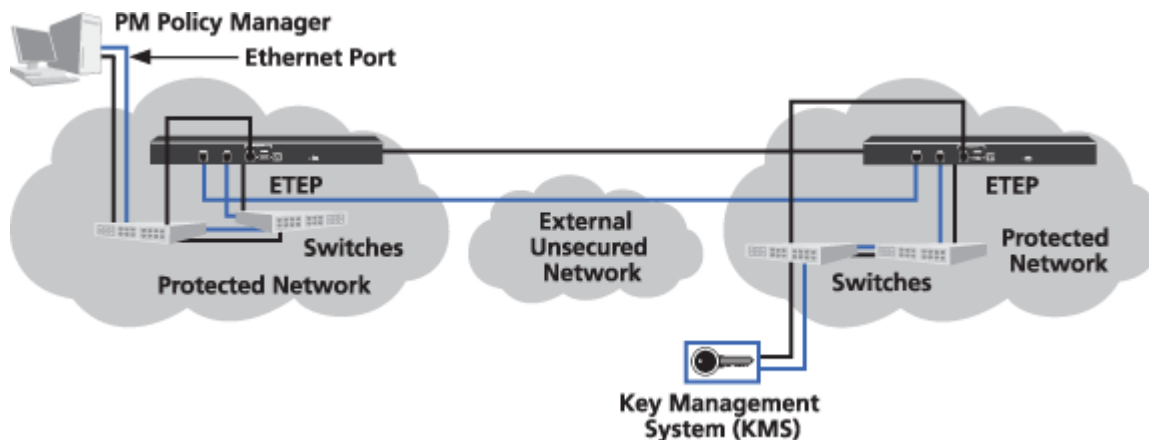
ETPM and ETKMS in Layer 3 IP Policies

With larger IP networks, the ETPM and the external ETKMSs could be located on different subnetworks, as shown in [Figure 8](#). When managing the ETPM and ETKMS in-line, the communications path between the devices must pass through one or more PEPs and potentially one or more firewalls. For in-line management, in which management traffic can flow through the data path, be sure that the **Enable passing TLS traffic in the clear** feature is selected on all PEPs. Enable this feature from the ETEMS Appliance editor. By default, the Layer 3 PEPs are configured to pass all TLS traffic (port 443) in the clear.

NOTE

The **Enable passing TLS traffic in the clear** feature passes all TLS traffic in the clear for all destination addresses. For added security, disable **passing TLS traffic in the clear** and create a policy for all TLS traffic (port 443) between EncrypTight components. For more information on creating policies, see [“Creating Distributed Key Policies”](#) on page 181.

Figure 8 In-line ETKMS management in an IP network



ETPM and ETKMS in Layer 2 Ethernet Policies

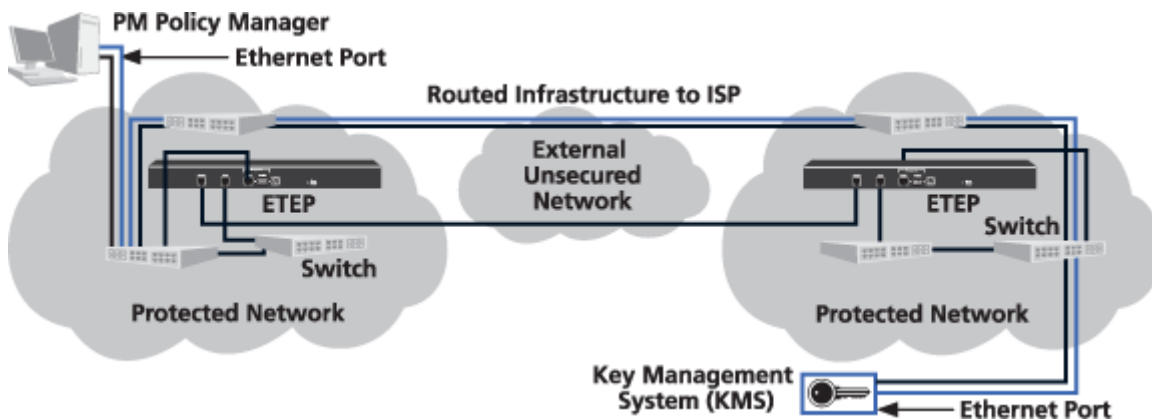
With Ethernet networks, you use Layer 2 PEPs. As with IP networks, when managing the ETPM and external ETKMS in-line the communications path between the devices must pass through one or more PEPs and potentially one or more firewalls. For in-line management with Layer 2 PEPs be sure that the **Enable passing TLS traffic in the clear** feature is selected in the ETEMS Appliance editor.

If you need to pass additional traffic in the clear, such as routing protocols, you can route the management communications using out-of-band connections or put your management traffic on a separate VLAN.

If you choose to put the management traffic on a separate VLAN, you will need to create a Layer 2 policy to pass packets with this VLAN tag in the clear. To prevent an interruption in management traffic, set the policy’s key renewal/lifetime to zero, so that the policy does not expire.

With out-of-band management, the management traffic between the ETPM and ETKMS is routed over a separate network path through the ISP. When the communications path passes through any firewalls, be sure to configure the firewall to pass TLS traffic. [Figure 9](#) shows an out-of-band management scenario with the ETPM connecting to an external ETKMS with Layer 2 PEPs encrypting Ethernet data.

Figure 9 Out-of-band ETKMS management in an Ethernet network



External ETKMS to ETKMS Connections

ETKMSs must be able to communicate with each other in two situations:

- Backup ETKMSs are used for redundancy
- Multiple ETKMSs share policy information and keys to distribute to the PEPs that they control

This section addresses the connections between two or more external ETKMSs. If you also use a local ETKMS, the basic principles discussed here still apply.

If the ETKMSs are on the same subnetwork, the ETKMS to ETKMS interconnection is straightforward. ETKMSs communicate with each other using the Ethernet ports on each ETKMS. For large, dispersed networks, multiple ETKMSs must be able to share keys with each other. The connections between ETKMSs depend on the network type: IP network or Ethernet network.

This section includes the following topics:

- [“Connections for Backup ETKMSs” on page 29](#)
- [“Connecting Multiple ETKMSs in an IP Network” on page 30](#)
- [“ETKMS to ETKMS Connections in Ethernet Networks” on page 30](#)

Connections for Backup ETKMSs

In some EncrypTight configurations a pair of ETKMSs, a primary ETKMS and a secondary ETKMS, are used to provide network redundancy. The ETPM distributes the policies to both the primary ETKMS and backup ETKMS. Only the primary ETKMS distributes the keys and policies to the PEPs. If the backup ETKMS detects a communication failure with the primary ETKMS due to a ETKMS failure or network failure, the backup ETKMS assumes the generation and distribution of the keys and policies to the PEPs. Once communication with the primary ETKMS is reestablished, the primary resumes the distribution of the keys and policies to the PEPs.

Backup ETKMSs should be external ETKMSs. Using a local ETKMS as a backup ETKMS is not recommended. If you use backup ETKMSs, the backup ETKMS must be able to check the status of the primary ETKMS so that it can take over operations in the event of a communication failure. It is recommended that you locate the backup ETKMS and the primary ETKMS together. The primary and backup ETKMSs communicate using the Ethernet ports on each ETKMS.

Also keep in mind the following:

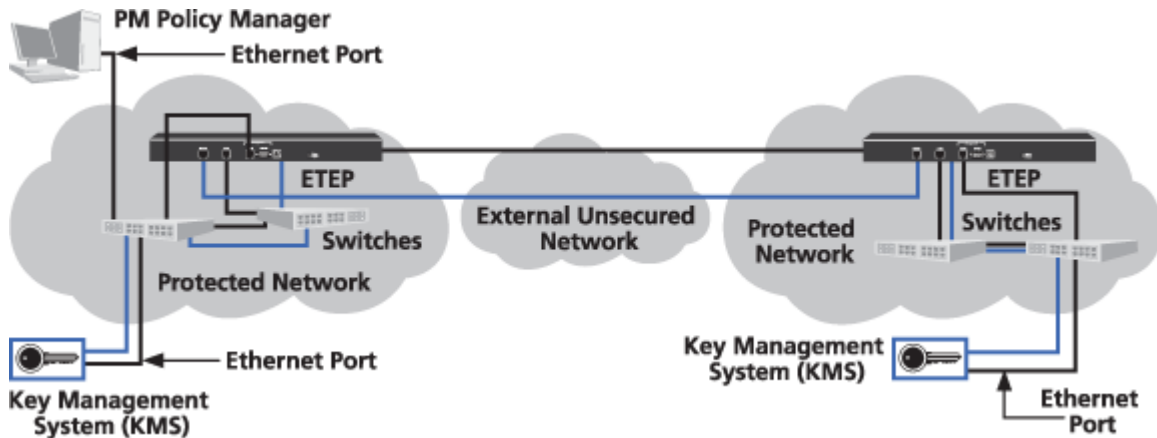
- Both the primary ETKMS and the backup ETKMS must be able to communicate with the same PEPs.
- Each ETKMS can only use one backup ETKMS. Similarly, each backup ETKMS can only serve as a backup to one ETKMS.
- Backup ETKMSs must use the same type of IP address as the primary ETKMS. For example, if the primary uses an IPv6 address, the backup ETKMS must use an IPv6 address.
- You do not explicitly add backup ETKMSs to the Appliance Manager in ETEMS and they are not listed in that window. Instead, you specify a backup ETKMS when you add a primary ETKMS in ETEMS, and only the primary ETKMS is listed in the Appliance Manager.

Connecting Multiple ETKMSs in an IP Network

Figure 10 shows two external ETKMSs located on different IP networks. Both ETKMSs are used as primary ETKMSs in a large, dispersed network.

When the ETKMSs are managed in-line, the communications path between the devices must pass through one or more PEPs and potentially one or more firewalls. By default, the Layer 3 PEPs pass all TLS traffic (port 443) in the clear. Be sure that the **Enable passing TLS traffic in the clear** feature is enabled for all PEPs which must pass TLS traffic. Enable this feature from the ETEMS Appliance editor.

Figure 10 In-line management of ETKMSs located on different IP networks



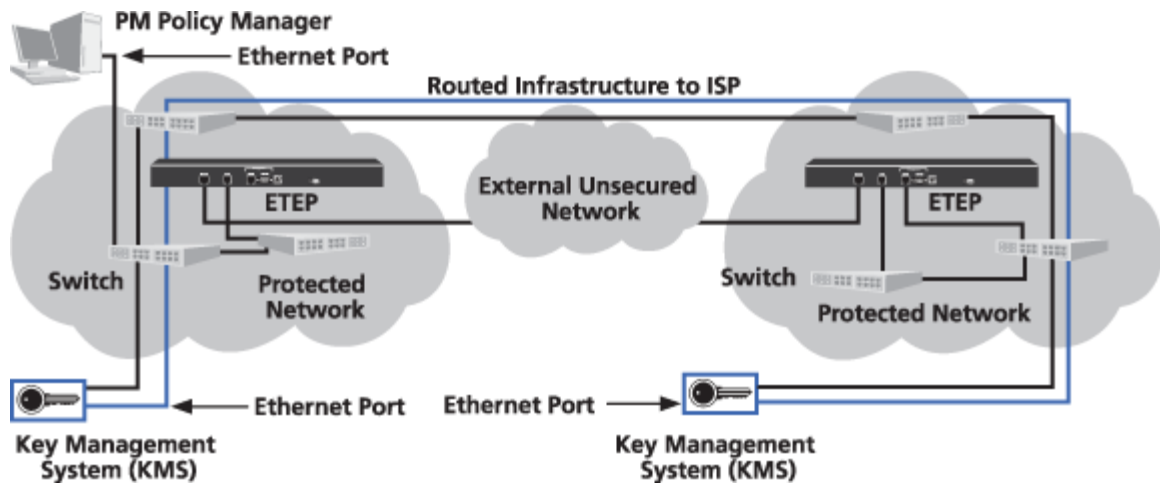
ETKMS to ETKMS Connections in Ethernet Networks

For in-line management when the ETKMSs are on different Ethernet networks, make sure that the **Enable passing TLS traffic in the clear** feature is enabled on the Layer 2 PEPs.

If you need to pass additional traffic in the clear, such as routing protocols, you can route the management communications using out-of-band connections or put your management traffic on a separate VLAN.

If you choose to put the management traffic on a separate VLAN, you will need to create a Layer 2 policy to pass the VLAN tag in the clear. To prevent an interruption in management traffic, set the policy’s key renewal/lifetime to zero, which means “do not expire or update.”

With out-of-band management, the management traffic between the ETKMSs is routed over a separate network path through the ISP. When the communications path passes through any firewalls, be sure to configure the firewall to pass TLS traffic. Figure 11 shows an out-of-band management scenario with the external ETKMS connecting to another external ETKMS, with Layer 2 PEPs encrypting Ethernet data.

Figure 11 Out-of-band management of ETKMSs located on different Ethernet networks

ETKMS to PEP Connections

The communications between the ETKMSs and the PEPs require a connection between the Ethernet ports on each ETKMS and the management port on each PEP. The ETKMS to PEP connections depend on the network type: IP network or Ethernet network.

This section addresses connections between external ETKMSs and the PEPs. If you also use a local ETKMS, the basic principles discussed here still apply. However, a local ETKMS runs on the same workstation as the ETPM. Therefore the communications between the local ETKMS and the PEPs require a connection between an Ethernet port on the management workstation and the management port on each PEP.

This section includes the following topics:

- [“ETKMS to PEP Connections in IP Networks” on page 31](#)
- [“ETKMS to PEP Connections in Ethernet Networks” on page 32](#)

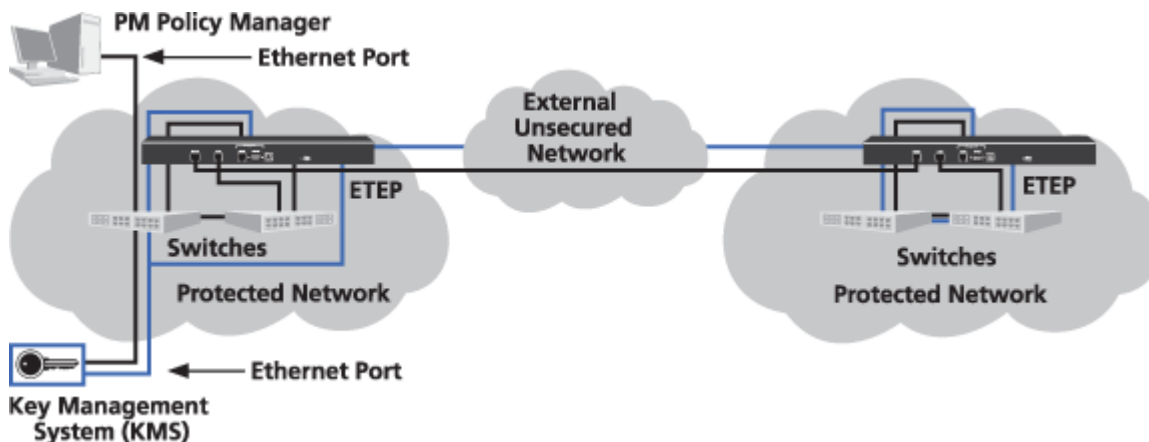
ETKMS to PEP Connections in IP Networks

[Figure 12](#) shows one external ETKMS connecting to two PEPs. The connections between the ETKMS and the first PEP co-located on the same network is a straightforward connection. The ETKMS’s Ethernet port connects through the internal protected network to the PEP’s management port.

When managing in-line, the connection between the ETKMS and the second PEP located on a different network must pass through the data ports on both PEPs to get to the management port on the second PEP.

To successfully pass management traffic, be sure that the **Enable passing TLS traffic in the clear** feature is enabled on all of the PEPs. By default, the Layer 3 PEPs pass all TLS traffic (port 443) in the clear. This option is configured on the Features tab of the ETEMS Appliance editor.

Figure 12 In-line ETKMS to PEP communications in IP networks



ETKMS to PEP Connections in Ethernet Networks

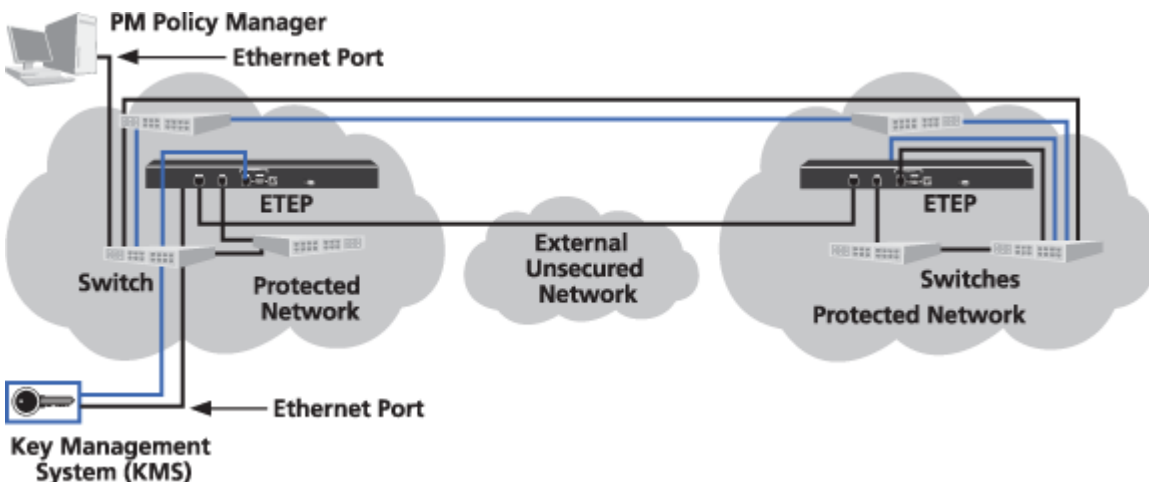
If the ETKMS and the PEP are located on the same subnetwork, the ETKMS to PEP interconnection is straightforward. For in-line management when the ETKMS and the PEP are located on different Ethernet networks, make sure that the **Enable passing TLS traffic in the clear** feature is enabled on the Layer 2 PEPs.

If you need to pass additional traffic in the clear, such as routing protocols, you can route the management communications using out-of-band connections or put your management traffic on a separate VLAN.

If you choose to put the management traffic on a separate VLAN, you will need to create a Layer 2 policy to pass the VLAN tag in the clear. To prevent an interruption in management traffic, set the policy’s key renewal/lifetime to zero, which means “do not expire or update.”

With out-of-band management, the management traffic between the ETKMSs and the PEPs is routed over a separate network path through the ISP. When communications paths pass through any firewalls, be sure to configure the firewalls to pass TLS traffic. [Figure 13](#) shows an out-of-band management scenario with the external ETKMS connecting to a PEP on a different subnetwork with Layer 2 PEPs encrypting Ethernet data.

Figure 13 Out-of-band ETKMS to PEP communications in Ethernet networks



Network Clock Synchronization



CAUTION

Failure to synchronize the time of all EncrypTight components can result in a loss of packets or compromised security.

EncrypTight requires that the clocks on all the system's components be synchronized. If the clocks are not synchronized, communications between the components can be delayed, which can prevent the system from working as planned.

For example, the keys on the PEPs all have an expiration time. The ETKMSs must generate new keys and policies prior to that expiration time in order to prevent a lapse in security or loss of network data. In addition, PEPs that implement the same policy require matching sets of keys for communications to occur. If one PEP's keys expire before another PEP's keys or if one PEP's keys become active before another PEP's keys, packets can be improperly dropped or passed in the clear.

It is essential that ETPM, ETKMS, and PEPs are synchronized to the same time source.

- Configure the workstation running EncrypTight to synchronize with a corporate time server within your network or with a public time server located somewhere on the Internet, or install a time service on the management station.
- External ETKMSs run on Linux servers that have Network Time Protocol (NTP) installed. Each of these ETKMSs can operate as an NTP server or an NTP client, or both. You can configure each ETKMS to synchronize with a timer server, or you can configure the ETPM, ETKMSs and PEPs to synchronize with one of the ETKMS servers.
- The PEPs include a Simple Network Time Protocol (SNTP) client, which can connect to an NTP server. The PEP SNTP client supports unicast client mode, in which the client sends a request to the designated NTP server and waits for a reply from the server.

You can check the current time of your PEPs in the ETEMS Appliance Manager. Refresh the status of the appliances and then view the Date/Time column (you may need to resize the columns).



NOTE

- *After you enable SNTP on ETEP PEPs and push the configuration, the ETEP PEPs immediately synchronize with the NTP server.*
- *If you re-provision a PEP that has been out of service, it is recommended that you synchronize the appliance with an NTP server and reboot it before you attempt to use the PEP with either ETEMS or ETPM. For more information on using SNTP, see the configuration chapter for your PEP.*

IPv6 Address Support

EncrypTight supports using both IPv4 and IPv6 addresses for the ETKMS and the management port of the ETEPs, as well as on the management workstation. The IPv6 standard was developed to provide a larger address space than the IPv4 standard and is intended to replace it as the IP addresses that are available with the older standard are exhausted. IPv6 addressing also provides other benefits, such as more efficient routing.

IPv6 addresses are 128-bit addresses consisting of eight hexadecimal groups that are separated by colons, followed by an indication of the prefix length. Each group is a 4-digit hexadecimal number. The hexadecimal letters in IPv6 addresses are not case sensitive.

The prefix length is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address. The decimal value is preceded by a forward slash (/). Valid values are 0-128 inclusive.

IPv6 addresses are typically composed of two logical parts: a network prefix (a block of address space, like an IPv4 subnet mask), and a host part. The prefix length indicates the number of bits used for the network portion of the address.

The following is an example of an IPv6 address with a 64-bit prefix:

```
2001:0DB8:0000:0000:0211:11FF:FE58:0743/64
```

IPv6 representation can be simplified by removing the leading zeros in any of the hexadecimal groups. Trailing zeroes may not be removed. Each group must include at least one digit.

IPv6 addresses often contain consecutive groups of zeros. To further simplify address entry, you can use two colons (::) to represent the consecutive groups of zeros when typing the IPv6 address. You can use two colons (::) only once in an IPv6 address.

Table 2 IPv6 address representations

Address Format	Address Representation
Full format	2001:0DB8:0000:0000:0211:11FF:FE58:0743
Leading zeroes dropped	2001:DB8:0:0:211:11FF:FE58:743
Compressed format (two colons) with leading zeroes dropped	2001:DB8::211:11FF:FE58:743

If any of your ETEPs are configured with an IPv6 address on the management port, the ETKMSs and the management workstation must be assigned an IPv6 address or configured for dual-homed operation to support both IPv4 and IPv6 addresses. If the ETKMS software is configured with an IPv4 address only, it cannot initiate connections to ETEPs that have IPv6 addresses. ETPM will not allow you to deploy a policy that includes an IPv4 ETKMS and IPv6 ETEPs.

Certificate Support

You can secure the management communications in an EncrypTight deployment using Public Key Infrastructure (PKI) certificates. By default, communications between EncrypTight components use the TLS protocol, which encrypts the communications. If you enable strict authentication, the communications are also authenticated with digitally signed certificates.

To use strict authentication, you need to select a Certificate Authority (CA) from which you want to obtain signed certificates. Depending on the CA you choose and other factors such as the types of certificates you want to purchase, acquiring certificates can take as little as an hour or less, or several days.

This User Guide assumes you already have a relationship with a CA. If you do not already have an established relationship with a CA, acquiring CA-signed certificates can take longer. The CA that you choose can provide information regarding their process and what to expect, as well as the costs involved.

Another factor to consider if you plan to use certificates is the size of your EncrypTight deployment. Generating requests and installing certificates for a large number of appliances can take a considerable amount of time. Therefore, you need to plan for sufficient time to accomplish the necessary tasks.

In addition to strict authentication, EncrypTight supports the use of smart cards such as the DoD Common Access Card (CAC) to limit access to authorized personnel and to enhance auditing. When a smart card is used, EncrypTight uses certificates from the card in addition to the certificates you install. For more information about using smart cards with EncrypTight, see [“Using a Common Access Card” on page 294](#).

To learn more about working with certificates and strict authentication, see [“Using Enhanced Security Features” on page 261](#).

Network Addressing for IP Networks

With Layer 3 networks, EncrypTight can use one of three network addressing methods to specify the source IP address used in the encapsulated packet’s header:

Table 3 Network Addressing Options

Addressing Method	Description
Preserve network addressing of the protected network	Uses the original source IP address in the packet header. This is the default network addressing method.
Use the PEP’s remote port address	Replaces the original source IP address in the packet header with the PEP’s remote port IP address.
Use a virtual IP address	Replaces the original source IP address in the packet header with a virtual IP address specified in the network set.

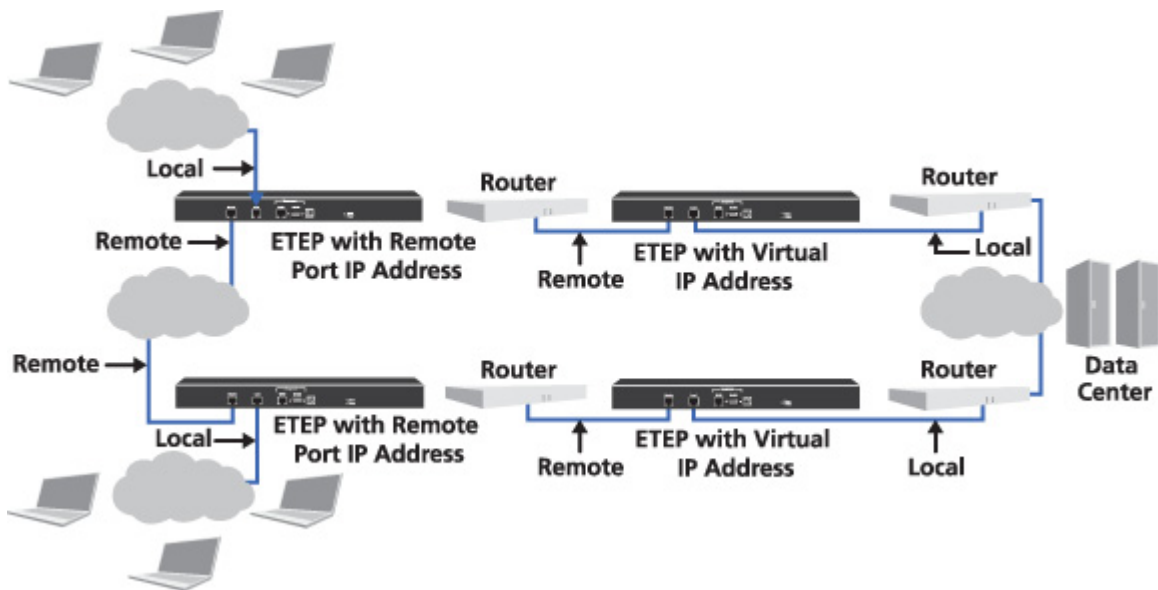
With most distributed key policies, you will preserve the network addressing of the protected networks, which is referred to as *transparent mode*. When you preserve the network addressing of the protected network, the encapsulated packets are routed to their proper destination without changing the routing tables within the WAN.

However, in certain situations you might want to conceal the original source IP address and replace it with either the IP address of the PEP’s remote port or a virtual IP address, which is referred to as *non-transparent mode*. For example, since private IP addresses cannot be routed over the internet, any traffic between private networks transmitted over the internet must use public IP addresses.

- If you need to route traffic through a specific PEP, use the PEP’s remote port IP address.
- For load balanced traffic, use a virtual IP address.

In the example shown in [Figure 14](#), traffic is being sent between a corporate data center and remote locations over a Layer 3 public internet. The traffic is encrypted using a policy defined in ETPM. The PEPs are configured to operate in non-transparent mode in order to hide the source IP address of the packets. The traffic to and from the data center is load balanced and therefore a virtual IP address is used on both data center PEPs (labeled #2 in [Figure 14](#)). The remote sites use a remote port IP address to force traffic through a specific PEP. The specified IP addresses appear in the encryption header rather than the original source IP address.

Figure 14 Using remote IP and virtual IP addresses to obscure the source address of the original packet



ETEP PEPs operate in transparent mode by default and no IP address is assigned to the local or remote ports. To use a remote port IP address or a virtual IP address, you need to disable transparent mode and assign the needed IP addresses when you add and configure the ETEP in ETEMS. With a virtual IP address, you also need to change the routing tables in the routers.

To use a virtual IP address as the source IP address:

- 1 Use ETEMS to disable transparent mode for the ETEP PEPs and configure the IP address settings for the local and remote ports.
- 2 Make sure the ETEP PEPs are configured to use Layer 3 encryption policies.
- 3 Use ETPM to configure the network sets to use virtual IP addresses. For information about creating network sets, see [“Managing Network Sets” on page 167](#).
- 4 Use the policy editor in ETPM to disable both of the Addressing Mode Override options in order to prevent the policy settings from overriding the virtual IP address settings. For more information about policy settings, see [“Policy Concepts” on page 181](#).
- 5 Verify that the WAN can direct the return traffic, destined for the virtual IP address, to the PEP’s remote port. A static route entry and a static ARP entry will need to be configured in the WAN router. For information on how to set up static routes, see the documentation for your router.

NOTE

Multicast network policies always preserve the network addressing of the protected networks.

Related topics:

- [“Adding a Network Set” on page 170](#)
- [“Addressing Mode” on page 185](#)
- [“ETEP Configuration” on page 299](#)

3 Installation and Configuration

This section describes how to install and configure EncrypTight for the first time, including:

- [Before You Start](#)
- [EncrypTight Software Installation](#)
- [Management Station Configuration](#)
- [Installing ETKMSs](#)
- [Configuring ETKMSs](#)
- [Policy Enforcement Point Configuration](#)
- [Default User Accounts and Passwords](#)
- [Managing Licenses](#)
- [Next Steps](#)

Before You Start

EncrypTight is a system that uses dedicated encryption devices referred to as Policy Enforcement Points (PEPs), a central server for distributing encryption keys (the Key Management System, or ETKMS), and a workstation running the management software.

- Install the EncrypTight software on a secure workstation.
- Install the ETKMS in a physically secure location and connect it to the network so that it can communicate with the management workstation and the PEPs.
- Install and configure the PEPs, usually at the point in your network where traffic is being sent to or from an untrusted network.

The EncrypTight software (version 1.9 and later) and the throughput speed of ETEPs with software version 1.6 and later are controlled by licenses. You must install a license for the EncrypTight software, and a license on each ETEP in your deployment. For more information, see [“Managing Licenses” on page 56](#).

This chapter provides instructions for these tasks. If you plan on using enhanced security options such as certificates, please refer to [“Using Enhanced Security Features” on page 261](#) for additional configuration instructions.

Before you install EncrypTight, review the following topics:

- [“Hardware Requirements” on page 38](#)

- “Software Requirements” on page 38
- “Firewall Ports” on page 39

Hardware Requirements

EncryptTight software can be installed on a Windows PC or laptop.

Table 4 EncryptTight management station requirements

Component	Requirements for the EncryptTight software
Operating System	Windows XP with SP3
CPU	3.0 GHz Pentium 4
RAM	512 MB
Hard disk space	165 MB
CD ROM drive	Read or read/write

Software Requirements

The third party software listed in [Table 5](#) is used in conjunction with EncryptTight to manage EncryptTight appliances. This software has been verified for use with EncryptTight and EncryptTight appliances.

Table 5 Third party management station software

Software	How it's used	Vendor
FTP server	Copies files to and from EncryptTight appliances, including log files and new firmware	Microsoft FTP server, included with Windows XP
SFTP server (optional: available with ETEP 1.6 and later)	Secures file transfers to and from EncryptTight appliances	Cerberus FTP Server 4 – Professional Edition
PDF reader	Opens the user documentation files on the product CD	Adobe Acrobat Reader version 6.0 or higher. Free download available from www.adobe.com .
SSH client (ETEPs)	Securely connects to the ETEP CLI	PuTTY, included with the ETEMS installation
Syslog server (optional)	Records log events to a syslog server	Kiwi Syslog Server version 7.2.20 or higher (installed as an application). Free download available from www.kiwisyslog.com .
Browser	Used to configure external ETKMSs	Internet Explorer 6.0 or higher, included with Windows XP

If any of your ETEPs are configured with IPv6 addresses on the management ports, the management workstation and the ETKMSs must also be configured with an IPv6 address. See the documentation for your operating system for information on how to enable support for IPv6 and IPv4 addresses.

Firewall Ports

In order for EncrypTight components to communicate, you need to make sure that any firewalls in your system are configured to allow the following protocols.

Table 6 Firewall ports

Protocol	Port	Comments
FTP	TCP 20, 21	Used for upgrading the software on a PEP.
HTTP	TCP 80	Used to communicate management information to EncrypTight appliances when TLS is disabled.
ICMP/Ping		Used to check connectivity with a device.
IPsec ESP	IP protocol 50	Used in encryption policies.
SFTP	TCP 22	Used for secure FTP operations.
SNMP	UDP 161, 162	Used to send SNMP traps from the PEPs to a management workstation.
SNTP	UDP 123	Used for time synchronization among EncrypTight components.
SSH	TCP 22	Used to securely access the CLI on ETEP PEPs and the ETKMS.
Syslog	UDP 514	Used to send syslog messages from the PEPs to a syslog server.
TLS (HTTPS)	TCP 443	A secure method of communicating management information between ETEMS and the PEPs.
XML-RPC	TCP 443	Used for communications between ETPM and the ETKMSs and between the ETKMSs and the PEPs.

EncrypTight Software Installation

EncrypTight installation tasks are described in the following topics:

- [“Installing EncrypTight Software for the First Time” on page 39](#)
- [“Upgrading to a New Version of EncrypTight” on page 40](#)
- [“Uninstalling EncrypTight Software” on page 40](#)
- [“Starting EncrypTight” on page 40](#)
- [“Exiting EncrypTight” on page 41](#)

Installing EncrypTight Software for the First Time

To install EncrypTight for the first time, follow the procedure below.

To install the EncrypTight software:

- 1 Quit all programs before installing EncrypTight.
- 2 Insert the EncrypTight CD into the CD-ROM drive. The installation program should start automatically. If it does not, open the CD and double click `EncrypTight.exe`.
- 3 Follow the instructions in the installation wizard. Click **Next** to advance through the wizard.
- 4 When the installation is complete, click **Done** to quit the installer.

 **NOTE**

It is strongly recommended that you synchronize the workstation hosting the EncrypTight software with an NTP server either on your network or on the Internet. For EncrypTight to function properly, all of the elements of EncrypTight need to synchronize with NTP servers.

Related topics:

- [“Uninstalling EncrypTight Software” on page 40](#)
- [“Installing Software Updates” on page 73](#)
- [“Network Clock Synchronization” on page 33](#)

Upgrading to a New Version of EncrypTight

Prior to upgrading to a new version of EncrypTight, uninstall the previous version (see [“Uninstalling EncrypTight Software” on page 40](#)). Previously installed third party software should be unaffected by an upgrade of EncrypTight.

To learn how to preserve and transfer your appliance and policy data if you are upgrading from ETEMS to EncrypTight, and for information about updating EncrypTight components to new versions, see [“Installing Software Updates” on page 73](#).

Uninstalling EncrypTight Software

To uninstall EncrypTight:

- 1 If you use a local ETKMS, stop it before continuing. For more information, see [“Launching and Stopping a Local ETKMS” on page 45](#).
- 2 Exit the EncrypTight application.
- 3 In the Microsoft Windows Control Panel, click **Add or Remove Programs**.
- 4 From the list of programs, select **EncrypTight**. Click **Change/Remove**.
- 5 The uninstall wizard asks if you want to save the appliance configurations. If you plan to reinstall EncrypTight or upgrade to a new version, click **Yes** to save the workspace data for use in the new version. Workspace data includes appliance configurations, default configurations, and policy data. User accounts are also retained, but not Login preferences. If you select **No**, workspace data and user accounts are deleted during the uninstall process.

Preferences are not saved when EncrypTight is uninstalled, regardless of whether you opt to save the appliance configurations.

Starting EncrypTight

Only one user at a time can be logged in to EncrypTight. User authentication is enabled by default. Use the default userId and password to log in to EncrypTight the first time. You can then change the default account or disable user authentication.

To start ETEMS:

- 1 From the **Start** menu, select **All Programs > EncrypTight**.

- 2 In the Login screen, enter the UserId **admin** and Password **admin**. Note that the userId and password are case sensitive.
- 3 Click **Login**.

NOTE

EncrypTight allows a maximum of three login attempts. After three unsuccessful login attempts, the EncrypTight software closes and must be restarted.

Related topic:

- [“Managing EncrypTight Users” on page 61](#)
- [“Using a Common Access Card” on page 294](#)
- [“Getting Started with ETEMS” on page 83](#)

Exiting EncrypTight

Exiting EncrypTight terminates the application. The EncrypTight appliances continue to operate as configured, regardless of whether EncrypTight is open. To prevent unauthorized users from accessing appliances, exit EncrypTight when the application is unattended or not in use.

Local and external ETKMSs, as well as all PEPs, continue to run even when the EncrypTight application is closed.

To exit EncrypTight:

- On the **File** menu, click **Exit**.

Management Station Configuration

The section includes the following topics:

- [“Securing the Management Interface” on page 42](#)
- [“Enabling the Microsoft FTP Server” on page 42](#)
- [“Configuring the Syslog Server” on page 43](#)

Securing the Management Interface

EncrypTight provides the methods listed in [Table 7](#) for encrypted and unencrypted communications between the management PC and the appliance's management port.

Table 7 ETEMS communications options

Option	Description
TLS	TLS (HTTPS) is used to encrypt communications between ETEMS and the appliance. TLS is enabled by default in EncrypTight. No additional software or configuration is required.
SSH	Provides secure remote access to the appliance CLI from the management PC. Available on ETEP appliances. An SSH client is included with EncrypTight. No additional configuration is required.

Consider the following items before choosing a method for securing management communications:

- HTTP is unavailable on ETEP appliances. If you disable TLS, ETEMS will be unable to communicate with ETEP appliances.
- You can enable IPsec on ETEPs with software version 1.6 or newer to establish secure communications to specific hosts.

Enabling the Microsoft FTP Server

EncrypTight uses FTP server software running on the management station to perform software upgrades on appliances and to extract appliance log files for viewing in ETEMS. This version of EncrypTight has been qualified with the Microsoft FTP server, which is included with the Windows XP operating system.

If you choose to use an SFTP server, refer to the documentation for your server software to learn about configuration options.

The following procedures describe how to enable the Microsoft FTP server and set up a new user. Prior to performing these tasks, check with your Windows administrator for information and restrictions specific to your organization's network.

To enable the Microsoft FTP Server service:

- 1 In the Control Panel, click **Add or Remove Programs**.
- 2 Click **Add/Remove Windows Components**.
- 3 Select **Internet Information Services (IIS)**.
- 4 Click **Details**.
- 5 Select **File Transfer Protocol (FTP) Service**, and then click **OK**.
- 6 Click **Next** to start the Windows Component Wizard.

To create a user on the management station for the FTP client to access:

- 1 In Windows Explorer, right-click **My Computer** and select **Manage**.
- 2 Expand **Local Users and Groups**.
- 3 Select **Users** and right-click.
- 4 Select **New User** to define the user name and password.

Configuring the Syslog Server

The EncryptTight appliance can be configured to send log messages and events to a syslog server on the management PC or other device. First, install the Kiwi Syslog Daemon as an application and follow the documentation provided with the product for initial configuration.

After you have installed the syslog daemon, use ETEMS to configure the appliances to send log messages to the syslog server. See the configuration chapter for your appliance model for more information about configuring syslog servers and log events.

Installing ETKMSs

Install the ETKMS server in a physically secure location. This server should be dedicated to the ETKMS functionality and requires the following external connections:

Table 8 ETKMS server connections

Connection	Description
System Power	Connect the system power to a grounded electrical source. An uninterrupted power supply (UPS) is recommended.
Mouse	You can use a USB or PS2 mouse. A USB mouse can connect to either of the two USB ports on the front panel or either of the two USB ports on the rear panel. A PS2 mouse connects to the mouse connector on the rear panel.
Keyboard	You can use a USB or PS2 keyboard. The USB keyboard can connect to either of the two USB ports on the front panel or either of the two USB ports on the rear panel. A PS2 keyboard connects to the keyboard connector on the rear panel.
Monitor	Connect the monitor to the video connector on the front or rear panel.
Network connection (eth0)	eth0 is the Linux designation for the Ethernet connection with a path to the management workstation containing the ETPM and to the PEPs' management ports. eth0 is normally configured to the Gb1 connector on the rear panel.
Network connection (eth1)	eth1 is inactive and unavailable by default.

NOTE

The mouse and keyboard are required only for the initial system configuration and can be disconnected after you complete the ETKMS installation.

ETKMSs are shipped with a factory default IP address of 192.168.1.3.

Configuring ETKMSs

Although some of the essential configuration of a ETKMS is the same for both local ETKMSs and external ETKMSs, the procedures for configuring each are different. For this reason, the basic configuration of a local ETKMS is discussed separately.

This section includes the following topics:

- [“Basic Configuration for Local ETKMSs” on page 44](#)
- [“Configuring External ETKMSs” on page 46](#)
- [“Configuring Syslog Reporting on the ETKMSs” on page 54](#)

Basic Configuration for Local ETKMSs

The basic configuration of a local ETKMS includes assigning an IP address and launching the ETKMS software.

This section includes the following topics:

- [“About Local ETKMSs” on page 44](#)
- [“Adding a Local ETKMS” on page 44](#)
- [“Launching and Stopping a Local ETKMS” on page 45](#)
- [“Starting the Local ETKMS Automatically” on page 45](#)

About Local ETKMSs

Local ETKMSs are intended for use with small to medium networks with no more than 10 nodes. When you use a local ETKMS, the ETKMS software runs on the same workstation as the EncrypTight software. Keep in mind the following information:

- Although the EncrypTight application does not need to remain open, the ETKMS software needs to run continuously in order to renew keys and refresh policies. For this reason, install the EncrypTight software on a reliable workstation. In addition, disable the Windows standby and hibernation modes. The local ETKMS software cannot renew keys and refresh policy lifetimes if the workstation enters standby or hibernation mode.
- It is strongly recommended that you assign a static IP address to the local ETKMS. If the local ETKMS IP address does not match the management station IP address, an error is generated when you attempt to launch the local ETKMS. You can use either an IPv4 address or an IPv6 address.
- Local ETKMSs use the time and date settings in effect on the workstation on which the EncrypTight software is installed. Because EncrypTight is dependant on network-wide clock synchronization, it is strongly recommended that you set up the management workstation to synchronize with an NTP server rather than setting the date and time manually. You should use the same time service for the EncrypTight workstation and the PEPs.
- You cannot run web server software on the same workstation as the EncrypTight software. The ETKMS application must use port 443. When a web service is running on the workstation, an error message appears in the ETKMS window.

To stop the Windows XP web service, click **Control Panel > Administrative Tools > Internet Information Services**. Click the **Web Sites** folder, and stop the Default Web Site service. To stop another web service that is running or to configure it to use a different port, see the documentation for the web service.

Adding a Local ETKMS

You add a local ETKMS in the ETEMS Appliance Manager. The IP address must be the IP address of the workstation on which EncrypTight is installed.

To add a local ETKMS:

- 1 In the Appliance Manager, click **File > New**.
- 2 In the New Appliance editor, from the **Product Family** box, select **ETKMS LM**.
- 3 From the **Software Version** box, select the appropriate software version.
- 4 In the **Appliance Name** box, enter a name for this local ETKMS.
- 5 In the **IP Address** box, enter the IP address of the workstation on which EncryptTight is installed. The address can be either an IPv4 address or an IPv6 address.
- 6 Click **Save**.

Related topics:

- [“Launching and Stopping a Local ETKMS” on page 45](#)
- [“Starting the Local ETKMS Automatically” on page 45](#)

Launching and Stopping a Local ETKMS

When you launch a local ETKMS, the ETKMS software runs as a separate application in a command line window on the management workstation. If the management workstation running the local ETKMS restarts, you must relaunch the local ETKMS.

To launch a local ETKMS:

- 1 In the Appliance Manager, select the local ETKMS.
- 2 Click **Tools > Launch ETKMS LM**.

The ETKMS software starts and opens a command line window.

To stop a local ETKMS:

- 1 Switch to the command line window in which the local ETKMS is running.
- 2 Press **CTRL + C**.
- 3 Type **Y**.

Related topic:

- [“Starting the Local ETKMS Automatically” on page 45](#)

Starting the Local ETKMS Automatically

EncryptTight ships with a batch file that you can configure to start the local ETKMS automatically when a user logs in the management PC. This eliminates the need to launch EncryptTight to start the local ETKMS.

The batch file, named `start.bat`, is included on the EncryptTight software CD. The batch file starts the local ETKMS when you log in to the management PC and stops it when you log out or the PC is powered off.

Changes to the local ETKMS configuration or EncrypTight software may necessitate changes to the batch file, as described in [Table 9](#).

Table 9 Maintaining the start.bat file

Type of change	Action
Upgrade to a new version of EncrypTight	No action required.
Change the ETKMS LM name or IP address in ETEMS	Modify the batch file variables to match the new ETKMS configuration.
Permanently uninstall EncrypTight	Manually delete <code>start.bat</code> from the PC. It is not removed by the uninstall program.
Discontinue using a local ETKMS	Delete the <code>start.bat</code> file from the PC.

Prior to configuring the batch file do the following:

- 1 Add a ETKMS LM in ETEMS (see [“Adding a Local ETKMS” on page 44](#)).
- 2 Launch the local ETKMS (**Tools > Launch ETKMS LM**). Successfully launching the local ETKMS demonstrates that the IP address is configured correctly and that there are no conflicting services running on the management station.

After launching the local ETKMS, configure the batch file to start the ETKMS automatically.

To configure the batch file:

- 1 Open the `start.bat` file in a text editor and modify the variables described in [Table 10](#).
- 2 Save the file and copy it to the `\Programs\Startup` folder for the management PC user. A typical path might be something like this:
`C:\Documents and Settings\username.domainname\Start Menu\Programs\Startup\.`

The next time that you log in to the management PC, the ETKMS software will start and open a command line window.

Table 10 Local ETKMS Batch file variables

Variable	Description
<code>installDir</code>	The EncrypTight installation directory. The default path is <code>C:\Program Files\EncrypTight</code> .
<code>Name</code>	The name as configured in ETEMS.
<code>IpAddress</code>	The IP address as configured in ETEMS

Related topics:

- [“About Local ETKMSs” on page 44](#)
- [“Adding a Local ETKMS” on page 44](#)
- [“Launching and Stopping a Local ETKMS” on page 45](#)

Configuring External ETKMSs

The minimum required steps to configure an external ETKMS include configuring the network connection (which includes the IP address and hostname) and specifying an NTP server for time synchronization.

This section includes the following topics:

- [“Logging Into the ETKMS” on page 47](#)
- [“Changing the Admin Password” on page 47](#)
- [“Changing the Root Password” on page 48](#)
- [“Configure the Network Connection” on page 49](#)
- [“Configure Time and Date Properties” on page 51](#)
- [“Starting and Stopping the ETKMS Service” on page 53](#)
- [“Checking the Status of the ETKMS” on page 54](#)
- [“Secure the Server with the Front Bezel” on page 54](#)

Logging Into the ETKMS

To configure the ETKMS, you must connect the monitor, keyboard, and mouse and log into the server directly.

The ETKMS has two default user accounts, admin and root. The default password for the **admin** account is **admin**. The default password for the **root** user is **password**. You can use the admin account to log into the ETKMS remotely using SSH for troubleshooting and management purposes. The root user can only log into the ETKMS directly. You must log in as root to configure the ETKMS.

To maintain the security of your system and networks, it is strongly recommended that you change the default admin password and the default root password as one of your first tasks, and periodically after that.

To log into the ETKMS:

- 1 At the login prompt, enter a user name and press **Enter**.
- 2 At the Password prompt, enter the password and press **Enter**.

Related topics:

- [“Changing the Admin Password” on page 47](#)
- [“Changing the Root Password” on page 48](#)

Changing the Admin Password

The first time you log into the ETKMS as admin, you must change the password. Changing the default admin password is an essential step in maintaining the security of the ETKMS and EncrypTight. After that first log in, use the following procedure to change the admin password.

To change the admin password:

- 1 Log in as admin.
- 2 Type **passwd** and press **Enter**.
- 3 At the prompt, type the current password and press **Enter**.
- 4 At the prompt, type the new password and press **Enter**.

It is recommended that the new password must be at least six characters long, contain a sufficient number of different characters, and must not be a common dictionary word.

- 5 At the prompt, retype the new password and press **Enter**.

6 Type **exit** to log out from the admin account.

For example:

```
Localhost login: admin

Password:

[admin@localhost ~] $ passwd

(current) UNIX password:

New UNIX password:

Retype new UNIX password:

passwd: all authentication tokens updated successfully.

[admin@localhost ~] exit
```

Related topics:

- [“Logging Into the ETKMS” on page 47](#)
- [“Changing the Root Password” on page 48](#)

Changing the Root Password

It is strongly recommended that you change the default root password when you initially set up the ETKMS server. It is recommended that the new password for the root user be at least eight characters long and contain a variety of different characters. Passwords are case sensitive and can include spaces. Do not use common words or phrases. You can use all printable keyboard characters and symbols. To create a strong password, consider the following:

- Use at least one uppercase and at least one lowercase alphabetic character.
- Use at least one numeric digit.
- Use at least one non-alphanumeric symbol.

The default password for the root user is **password**.

To change the root password:

- 1 Log in as root.
- 2 Type **passwd** and press **Enter**.
- 3 Follow the prompts to change the root password.

Remain logged in as root to complete the ETKMS configuration.



CAUTION

Keep track of the passwords you assign. If you lose these passwords, you can lose the ability to communicate with and manage the ETKMS. In some cases, restoring the unit to working order can require factory service.

- [“Logging Into the ETKMS” on page 47](#)
- [“Changing the Admin Password” on page 47](#)

Configure the Network Connection

The eth0 connection is the network connection with a path to the management workstation running ETPM and to the PEPs' management port. The eth1 connection is inactive and unavailable. Set the network connection as required by your network configuration, but it is recommended that you set a static IP address. You can assign both an IPv4 address and IPv6 address, if needed.

NOTE

If any of your ETEPs are configured with IPv6 addresses, you must configure the ETKMS and the management workstation to use an IPv6 address instead of, or in addition to, an IPv4 address. If the ETKMS software is configured with an IPv4 address only, it cannot initiate connections to ETEPs that have IPv6 addresses. ETPM will not allow you to deploy a policy that includes an IPv4 ETKMS and IPv6 ETEPs.

IPv4

Setting up the network connection requires running two scripts.

To configure the network connection and hostname:

- 1 At the command prompt, type **system-config-network**.
- 2 Tab to the **Edit Devices** option and press **Enter**.
- 3 Tab to the **eth0** device and press **Enter**.
- 4 Make sure that DHCP is not selected (use the spacebar to clear any selection) and then enter the:
 - **Static IP**
 - **Netmask**
 - **Default Gateway IP address**
- 5 Tab to **OK** and press **Enter**.
- 6 Tab to **Save** and press **Enter**.
- 7 Tab to **Edit DNS configuration** and press **Enter**.
- 8 Enter the **Hostname**, **Primary DNS**, **Secondary DNS**, and **Search** information.
- 9 Tab to **OK** and press **Enter**.
- 10 Tab to **Save & Quit** and press **Enter**.
- 11 At the command prompt, type **/opt/etkms/bin/etc-hosts-config.sh** and press **Enter**.
- 12 At the command line, restart the network service by typing **service network restart** and press **Enter**.
- 13 At the command line, restart the ETKMS service by typing **service etkms restart** and press **Enter**.

Verify the IP Address and Hostname Changes

You can use the following commands to verify the IP address and hostname changes:

- At the command line, type **ifconfig** and press **Enter** to view the IP address.
- At the command line, type **hostname** and press **Enter** to view the full hostname, such as `serv4.company.com`.
- Type **hostname -s** and press **Enter** to view the short hostname. In this example, if the full hostname is `serv4.company.com`, the short name is `serv4`.

IPv6

Setting up the network connections to use IPv6 addresses requires modifying several files.

To configure the network interface:

- 1 Using a text editor of your choice, edit the file:
`/etc/sysconfig/network-scripts/ifcfg-eth0`
- 2 To add an IPv6 address, add the following lines:

```
IPV6INIT=yes  
IPV6ADDR=<IPv6 Address>
```

Where **<IPv6 Address>** is the IPv6 address that you want to assign to the ETKMS. If you are using an IPv6 address, you also need to edit the `etkmsParams.sh` file (see [“To specify the IPv6 address of the ETKMS in the parameters script:” on page 50](#)).

- 3 Save and close the file.

To specify the IPv6 address of the ETKMS in the parameters script:

- 1 Edit the file:
`/opt/etkms/bin/etkmsParams.sh`
- 2 Edit the `ETKMS_IP` parameter to add the IPv6 address of the ETKMS.
Do not make any other changes to this file.
- 3 Save and close the file.

To set the hostname and IPv6 default gateway address:

- 1 Edit the file:
`/etc/sysconfig/network`
- 2 For an IPv6 address, add the following lines:

```
NETWORKING_IPV6=yes  
IPV6_DEFAULTGW=<gateway address>
```

Where **<gateway address>** is the IPv6 address of the default gateway.

Whether you are using IPv4 or IPv6 addresses, if this ETKMS is a backup ETKMS, the hostname must be the same as the primary ETKMS with `backup` appended to the name. For example, the backup ETKMS for a primary ETKMS named `ETKMS1.mycompany.com` must be named `ETKMS1backup.mycompany.com`.

- 3 Save and close the file.

To set the default DNS server and configure the hosts file:

- 1 At the command prompt, type `system-config-network`.
- 2 Tab to **Edit DNS configuration** and press **Enter**.
- 3 Enter the **Hostname**, **Primary DNS**, **Secondary DNS**, and **Search** information.
- 4 Tab to **OK** and press **Enter**.
- 5 Tab to **Save & Quit** and press **Enter**.
- 6 At the command prompt, type `/opt/etkms/bin/etc-hosts-config.sh` and press **Enter**.
- 7 At the command line, restart the network service by typing `service network restart` and press **Enter**.

- 8 At the command line, restart the ETKMS service by typing `service etkms restart` and press **Enter**.

Verify the IP address and hostname changes (see [“Verify the IP Address and Hostname Changes”](#) on page 49).

NOTE

- *Make a note of the eth0 IP address and the hostname. You will need this information in order to add the ETKMS in ETEMS.*
- *It is strongly recommended that you set a static IP address and turn off DHCP. Do not use DHCP to obtain an IP address.*
- *If you are configuring a backup ETKMS, you must use the same type of IP address for the backup as you used for the primary. For example, if the primary ETKMS was assigned an IPv6 address, you must assign an IPv6 address to the backup.*
- *When you add the ETKMS in ETEMS, use the short hostname. For example, if the full hostname is etkms1.mycompany.com, the ETKMS name is etkms1. In addition, the ETKMS name is case sensitive.*

Related topics:

- [“Configure Time and Date Properties”](#) on page 51
- [“Check the Status of the Hardware Security Module”](#) on page 53
- [“Starting and Stopping the ETKMS Service”](#) on page 53

Configure Time and Date Properties

All EncrypTight components, including the ETKMS, should be synchronized with a time server, preferably the same time server. Configure the time and date properties and then check the status of the connection with the time source. You must be logged into the ETKMS as root to make these changes.

TIP

Before you configure the NTP service, you might want to use the Linux `date` command to set the system clock. If there is a large difference between the hardware clock and the NTP server, it can take significantly longer for the clock to synchronize with the server. You can learn about the Linux `date` command from many online sources.

To set the time zone:

- 1 Edit the file


```
/etc/sysconfig/clock
```
- 2 For the **Zone** value, specify the appropriate filename. Zone files are located in:


```
/usr/share/zoneinfo
```

 Include the parent directory in the entry (for example, `America/New_York`).
- 3 Save and close the file.

To set up time synchronization:

- 1 Edit the file:


```
/etc/ntp.conf
```

- 2 Replace the defaults with your preferred time server. You can specify multiple time servers and use either IPv4 or IPv6 addresses. For example, the new section should look similar to the following:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 192.168.2.22
```

- 3 Save and close the file.

- 4 To set up the NTP daemon to start every time the server starts, at the command line, type:

```
chkconfig ntpd on
```

Changes to the NTP settings do not take affect until you restart the NTP daemon or the entire server.

To restart the NTP daemon:

- 1 At the command line, type:

```
service ntpd restart
```

To check the time source connection status:

- 1 At the command line, type:

```
ntpq -p
```

The result of this command should be similar to the following:

remote	refid	st	t	when	poll	reach	delay	offset	jitter
=====									
*ns.unc.edu	129.6.15.28	2	u	222	512	37	25.160	-173753	83.394

The fields described in [Table 11](#) can help you determine if there is a time sync problem.

Table 11 ntpq -p command output

Field	Description
remote	IP address of the NTP server.
st (stratum)	A stratum value of 16 indicates a time synchronization failure.
when	Number of seconds since the last poll. This value should be less than or equal to the poll value. A “when” value that exceeds the “poll” value indicates a time sync problem.
poll	Polling interval in seconds. The “poll” value will be greater than the “when” value when the time server is synchronizing successfully.
jitter	A value of 4000.00 indicates a time synchronization failure.

The ETKMS server may initially report as unsynchronized. The synchronization may take several minutes. After multiple attempts, if the output of the **ntpq -p** command continues to indicate a time synchronization problem check the following:

- Verify that the NTP server IP address is a valid address
- If you are using a local NTP server, check to see if the NTP server is powered on
- Check for network problems that may prevent the ETKMS from reaching the NTP server

Related topics:

- [“Configure the Network Connection” on page 49](#)
- [“Check the Status of the Hardware Security Module” on page 53](#)
- [“Starting and Stopping the ETKMS Service” on page 53](#)

Check the Status of the Hardware Security Module

A Hardware Security Module (HSM) for the ETKMS is available. The HSM physically secures the encryption keys used for communications between EncryptTight components. Before installing and starting the ETKMS service, make sure that the HSM device driver is running. If the HSM device driver is not running, you need to start it before running the ETKMS service.

To check the HSM device driver status:

- 1 At the command line, type `hsmstate` and press **Enter**.

The results should be:

```
HSM device 0: HSM in NORMAL MODE. RESPONDING. Usage Level=0%
```

If the HSM driver is not running, you need to start it.

To start the HSM device driver:

- 1 At the command line, type `e8k start` and press **Enter**.

Related topics:

- [“Configure the Network Connection” on page 49](#)
- [“Configure Time and Date Properties” on page 51](#)
- [“Starting and Stopping the ETKMS Service” on page 53](#)

Starting and Stopping the ETKMS Service

The ETKMS runs as a service in Linux. Once the ETKMS is started, the ETKMS restarts after each reboot of the Linux server.

To start the ETKMS service:

- 1 At the command line, type:

```
service etkms start
```

To stop the ETKMS service:

- 1 At the command line, type:

```
service etkms stop
```

Related topics:

- [“Configure the Network Connection” on page 49](#)
- [“Configure Time and Date Properties” on page 51](#)
- [“Check the Status of the Hardware Security Module” on page 53](#)

Checking the Status of the ETKMS

You should check that the ETKMS service is running before you proceed to use EncrypTight.

To check the status of the ETKMS service:

- 1 At the command line, type:

```
service etkms status
```

Secure the Server with the Front Bezel

The bezel prevents access to the CD ROM drive, front panel USB ports, and power switch.

Black Box strongly recommends that you install the front system bezel, secure the bezel with the key provided, and store the key in a secure location. Refer to the server manufacturer's documentation about this feature.

Configuring Syslog Reporting on the ETKMSs

You configure syslog reporting on the ETKMS by editing the ETKMS properties file, `kdist.properties`. A complete discussion of all of the options for syslog reporting is beyond the scope of this manual. You can find more information from a variety of online resources. If you are using IPv6 addresses in your system, you need to make sure that the syslog server that you use also supports IPv6 addresses.

- On local ETKMSs, this file is located in `<InstallDir>\tools\kdist\bin` directory, where **InstallDir** is the directory in which you installed the EncrypTight software.
- On external ETKMSs, the file is located in the `/opt/etkms/conf` directory. You will need to log into the ETKMS as root in order to make changes to this file.

To configure syslog reporting on a ETKMS:

- 1 In a text editor, open the `kdist.properties` file.
- 2 Find the line near the beginning of the file that begins with:

```
log4j.rootLogger=ALL,R
```
- 3 Edit this line to read:

```
log4j.rootLogger=INFO, stdout, var, Syslog
```
- 4 Locate the section that begins with:

```
#Alternate logger using Remote Syslog server.
```
- 5 Uncomment the following lines by deleting the “#” symbols:

```
#log4j.appender.Syslog=org.apache.log4j.net.SyslogAppender
#log4j.appender.Syslog.Threshold=INFO
#log4j.appender.Syslog.layout=org.apache.log4j.PatternLayout
#log4j.appender.Syslog.ConversionPattern=%d [%t] %-5p %c{1} - %m%n
#log4j.appender.Syslog.SyslogHost=x.x.x.x.
#log4j.appender.Syslog.Syslog.Facility=USER
#log4j.appender.Syslog.FacilityPrinting=true
```
- 6 In the line:

```
log4j.appender.Syslog.SyslogHost
```

Replace `x.x.x.x` with the IP address or the hostname of the syslog server.

- 7 Save and close the file.
- 8 Shut down and restart the ETKMS:
 - On external ETKMSs, restart the ETKMS service by typing:


```
service etkms restart
```
 - On local ETKMSs, close the command line window for the ETKMS software and in the EncrypTight window, select **Tools > Launch ETKMS LM**.

Policy Enforcement Point Configuration

EncrypTight Policy Enforcement Points (PEPs) can be configured for Layer 2 or Layer 3/4 operation. Models include:

- ET0010A
- ET0010A
- ET1000A

In most cases, when you install and configure the PEPs, you do not need to make addressing changes or other routing changes. The PEPs implement a network mode ESP transport mechanism that preserves all header information. The entire original packet is encrypted and a copy of the original header is used as the header for the new packet. This allows the PEPs to operate transparently, without requiring changes to your existing network addressing. You should maintain your existing network gateways as configured. You should not configure the local port on a PEP as a gateway address.

To prepare the PEPs for operation with EncrypTight:

- Perform basic installation tasks.

Perform initial setup as directed in the PEP's *Installation Guide*. At a minimum, this consists of connecting cables to the PEP's communication ports and setting the management port IP address.

When they are first installed, ETEP PEPs pass all traffic in the clear until they receive policies. Refer to the documentation for your PEPs for more information on initial behavior and how to make sure the PEPs are properly installed.

If you plan to use a PEP with EncrypTight distributed key policies, you should not configure any other types of policies on the PEP before you enable EncrypTight. Doing so can have undesirable effects.
- Configure the appliances in the EncrypTight software.

Using the ETEMS Appliance Manager feature in EncrypTight, add and configure each PEP. Refer to the sections below for configuration settings that are required for distributed key and negotiated key policies.

 - For distributed key policies, see [“Adding a New PEP in ETEMS” on page 148](#)
 - For point-to-point negotiated policies, see [“Creating Layer 2 Point-to-Point Policies” on page 335](#)

Related topics:

- [“Provisioning Basics” on page 95](#)
- [“Adding a New PEP in ETEMS” on page 148](#)
- [“Creating Layer 2 Point-to-Point Policies” on page 335](#)

Default User Accounts and Passwords

Changing the default passwords for all of the EncrypTight components is an important step in maintaining the security of your network. This list is a reminder of the default passwords that you should change.

Table 12 Passwords to change

Component	Passwords
ETEP PEPs	Administrator password (admin) Network Manager/Ops password (ops)
ETKMSs	admin password Root password Keystore password, if you use certificates and strict authentication. The file is named etkms.keystore on an external ETKMS, and kdist.keystore on a local ETKMS.
ETEMS	Administrator password, if you enable User Authentication User account passwords, if you enable User Authentication

For instructions on how to change the passwords, see the documentation for each component.

Managing Licenses

The use and functionality of EncrypTight components are controlled through licenses. How the licenses work and the features available depend on the component.

NOTE

- Licenses are required for ETEPs with software version 1.6 and later. Previous versions of ETEP software do not require licenses.
- A license is required for EncrypTight 1.9 and later. Previous versions of the EncrypTight software do not require a license.

Each ETEP is capable of transmitting traffic at a range of speeds that varies by model. Licenses control the throughput speed. This allows you to upgrade your existing ETEPs to transmit traffic at higher speeds as your network grows and your needs change. [Table 13](#) lists the available speeds for each ETEP model. You can specify the throughput speed of the ETEP on the Interfaces tab in the appliance editor.

Table 13 ETEP Throughput Speeds

Model	Available Throughput
ET0010A	3, 6, 10, 25, 50 Mbps
ET0100A	100, 155, 250 Mbps
ET1000A	500, 650 Mbps, 1 Gbps

You need to install a license on each ETEP that you use. Licenses are linked to the serial number of the ETEP on which they are installed. You cannot install a license intended for one ETEP on a different ETEP.

Before you begin adding PEPs and using the EncryptTight software, contact Customer Support to acquire your license key (see [“Contacting Black Box Technical Support” on page 14](#)). You need to provide the EncryptTight ID. To view the EncryptTight ID, choose **Edit > License**.

If you upgrade from a command line-only installation to a full EncryptTight deployment, you can no longer use the command line-only license and must acquire an EncryptTight license.

You cannot install licenses on your ETEPs until you install a license for EncryptTight. The EncryptTight license specifies the maximum number of ETEPs that can be managed in your deployment and the speeds at which they are licensed to run. The license specifically controls how many ETEPs can be configured to run at each throughput speed. For example, one EncryptTight deployment might run 10 ET0100As at 100 Mbps and an additional four ET0100As at 250 Mbps. When your needs change, you can easily upgrade the EncryptTight software to support a larger number of ETEPs.

Related topics:

- [“Installing Licenses” on page 57](#)
- [“Upgrading Licenses” on page 58](#)

Installing Licenses

You install and update licenses using the License Manager.

To enter EncryptTight licenses:

- 1 In the Appliance Manager, choose **Edit > License**.
- 2 In the License Manager, click **Enter EncryptTight License**.
- 3 In the **EncryptTight License** box, type the license key, or copy and paste it.
- 4 Click **OK**.
- 5 Click **OK** to close the License Manager.

After you enter a license for EncryptTight, you can install licenses on your ETEPs. The ETEP license specifies the speed at which the ETEP can transmit traffic.

To install a license on the ETEP:

- 1 In the Appliance Manager, select the ETEPs on which you want to install licenses.
- 2 Choose **Tools > Put License**.

You can also install the license on the ETEP when you push configurations by selecting the **Put Throughput License** option.

 **NOTE**

- You can check to see if a license is installed and the throughput speed configuration by clicking **Tools > Compare Config to Appliance**.
- Be aware that CLI commands that affect the file system such as `restore-filesystem` will erase the currently installed license and you will need to re-install the license to regain full functionality.

Upgrading Licenses

When your needs change, you can easily upgrade the number of ETEPs that EncrypTight can manage and you can also upgrade your ETEPs to run at faster throughput speeds.

This section includes the following topics:

- [“Upgrading the EncrypTight License” on page 58](#)
- [“Upgrading ETEP Licenses” on page 58](#)

Upgrading the EncrypTight License

When you upgrade the EncrypTight license, a new license replaces the old one. Contact Customer Support to acquire a new license. When you receive the new license, follow the procedure for entering EncrypTight licenses (see [“To enter EncrypTight licenses:” on page 57](#)).

For information on how to contact Customer Support, see [“Contacting Black Box Technical Support” on page 14](#).

Upgrading ETEP Licenses

You can upgrade ETEP licenses in order to configure the ETEPs to run at faster throughput speeds. After you install a new EncrypTight license, use the same procedure for installing a license on the ETEP to upgrade the ETEPs. After installing the licenses, open the appliance editor for each affected ETEP and change the **Throughput Speed** to the new value. For more information about configuring ETEPs, see [“Provisioning Appliances” on page 95](#) and [“ETEP Configuration” on page 299](#).

You can upgrade the ETEP whenever you have unused licenses for speeds that a selected ETEP can support. Once a license for a specific throughput speed is installed on a specific ETEP it cannot be used on any other ETEP.

Next Steps

After the EncrypTight components have been installed, use ETEMS and ETPM to configure your PEPs and policies as summarized below. See the ETEMS and ETPM sections of this user guide for more information.

If you plan on using enhanced security options such as certificates, refer to [“Using Enhanced Security Features” on page 261](#) before you proceed.

- 1 In ETEMS, configure the ETKMSs and PEPs, and push the configurations to the PEPs.
- 2 In ETEMS, check the communications link and status of the ETKMSs.
- 3 In ETEMS, make sure all PEPs are synchronized in time. You can view the date and time in the Appliance Manager view.
- 4 If you are using external ETKMSs, log in to the web interface for each ETKMS and make sure that the time is in sync with the PEPs and the management workstation.
- 5 In ETPM, add the policy components such as networks or VLAN ID Ranges.

- 6 In ETPM, create your policies.
- 7 In ETPM, deploy the policies to the ETKMSs and PEPs.

4 Managing EncrypTight Users

This section includes the following topics:

- [Working with EncrypTight User Accounts](#)
- [Configuring EncrypTight User Authentication](#)
- [Managing EncrypTight Accounts](#)
- [Changing an EncrypTight User Password](#)
- [How EncrypTight Users Work with ETEP Users](#)

Working with EncrypTight User Accounts

This chapter discusses user accounts for the EncrypTight software. These accounts are unique to EncrypTight and should not be confused with user accounts on the appliance or external ETKMS.

EncrypTight is able to authenticate users when they start the application. This authentication check is intended to prevent an unauthorized person from adding, deleting, or modifying appliance configurations or policies. User authentication is enabled by default. When you first start EncrypTight, use the default user name **admin** and password **admin** to log in.

The following list summarizes how user accounts work:

- EncrypTight has two user types: administrator and user. The EncrypTight administrator controls access to the EncrypTight application by managing its users and passwords. The administrator can create, modify, and delete other users, while the user can change only its own password.
- User verification is enabled by default.
- An administrator account exists by default with the user name **admin** and password **admin**.
- You must have at least one administrator account. If you have only one administrator account, EncrypTight prevents you from deleting it until you create a replacement.
- Multiple user and administrator accounts are allowed. User names must be unique.
- When authentication is enabled, the default password expiration period is set to zero, which means “do not expire.”

Table 14 EncryptTight account types and privileges

Task	Administrator	User
Enable user ID/password authentication	Yes	No
Set password expiration period	Yes	No
Create EncryptTight users	Yes	No
Modify EncryptTight user names and passwords	Yes	No
Delete EncryptTight users	Yes	No
Change own password	Yes	Yes
Configure appliances and policies	Yes	Yes
View logs and performance statistics	Yes	Yes

 **NOTE**

If EncryptTight is managing ETEP 1.4 and later appliances, we recommend creating a user account in EncryptTight that matches the user name and password that you plan to use on the ETEP appliances. See [“How EncryptTight Users Work with ETEP Users” on page 67](#) for more information.

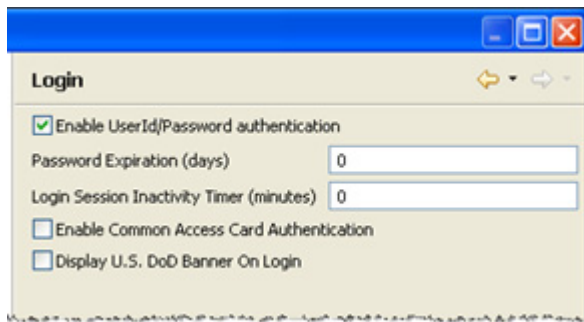
Related topics:

- [“Configuring EncryptTight User Authentication” on page 62](#)
- [“Managing EncryptTight Accounts” on page 65](#)
- [“Changing an EncryptTight User Password” on page 66](#)
- [“How EncryptTight Users Work with ETEP Users” on page 67](#)
- [“Appliance User Management” on page 102](#)

Configuring EncryptTight User Authentication

The EncryptTight administrator can set the following authentication preferences for EncryptTight users:

- User ID and password authentication
- Password expiration period
- Login session inactivity timer
- Common Access Card authentication
- US government login banner displayed upon application startup

Figure 15 Login preferences**To set login preferences:**

- 1 From the Edit menu, click **Preferences**.
- 2 In the Preferences window, expand the ETEMS tree and click **Login**.
- 3 In the Login area, configure the preferences. The options are described in the rest of this section.
- 4 Click **Apply** and then click **OK**.

Password Authentication and Expiration

User authentication is enabled by default. When authentication is enabled, the default password expiration period is set to zero, which means “do not expire.”

When using a finite password expiration period, the expiration date is set to the current date plus the number of expiration days. When the specified number of days elapses, the application notifies the EncrypTight user of the expiration and asks for an updated password. The password expiration field accepts values from 0–999999999.

Login Session Inactivity Timer

The login session inactivity timer lets you set a session timer for the EncrypTight software. When the time is set, the application is closed if no user activity is detected in the EncrypTight software in a specified amount of time.

As the timer approaches expiration, EncrypTight presents a warning message. If the message is acknowledged, the session timer resets. If the message is not acknowledged, the session terminates.

The timer is set to zero by default, which means that the session does not expire. The inactivity timer is specified in minutes, with valid values ranging from 0–10,080 minutes (168 hours).

The timer does not affect the local ETKMS, which continues to run regardless of whether the EncrypTight application is open.

Common Access Card Authentication

The administrator can also require that EncrypTight use a Common Access Card. When this is enabled, users must possess a Common Access Card to access the system and insert the card into the reader before they start EncrypTight. When EncrypTight opens:

- You are prompted for your EncrypTight user name.
- The software for the CAC reader will prompt you for your PIN.
- If user authentication is also enabled (the default setting), you are prompted for your EncrypTight user account password.

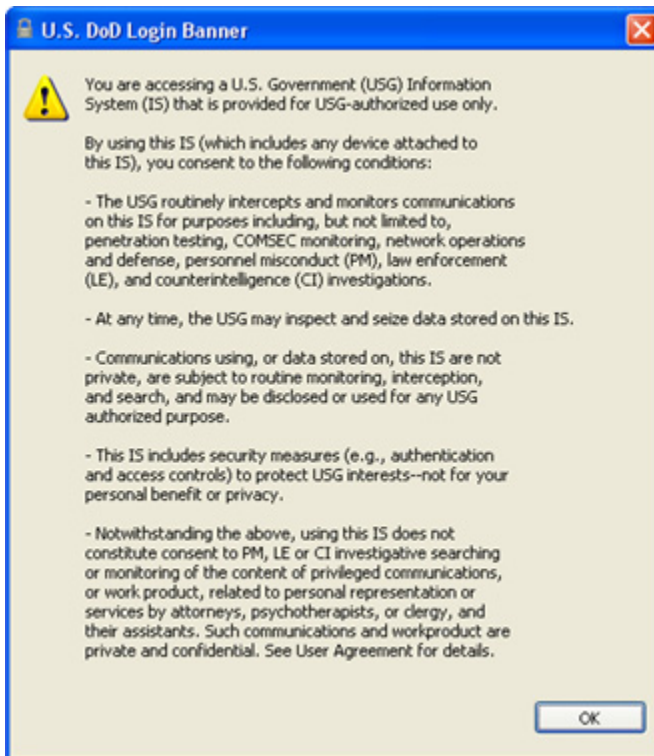
- If your EncrypTight deployment includes ETEPs running software version 1.6 or later, entering a password is optional.
- If your deployment includes ETEPs with software previous to 1.6, or other models of PEPs, you must enter a valid password.
- If user authentication is not enabled, you are logged into the system immediately.

This feature is used in conjunction with strict authentication in your EncrypTight deployment. To learn how to set up your system to use strict authentication with a Common Access Card, see [“Using a Common Access Card” on page 294](#).

U.S. DoD Login Banner

The U.S. DoD login banner contains the U.S. government-supplied text shown in [Figure 16](#). The login banner is disabled by default. When enabled, the login banner appears after a user enters the EncrypTight login credentials. A user must acknowledge the terms of usage to successfully log in. The banner text cannot be modified or replaced.

Figure 16 U.S. DoD login banner



Important Information about Login Preferences and Upgrades

When EncrypTight is uninstalled prior to upgrading to a new version, Login preferences are not saved. When you start the new version of EncrypTight you will need to reset your Login preferences if you use something other than the defaults. Default settings are shown in [Table 15](#).

Table 15 Login preferences default settings

Preference	Setting
User ID / Password Authentication	Enabled
Password Expiration	0
Login Session Inactivity Timer	0
Common Access Card Authentication	Disabled
U.S. DoD Login Banner	Disabled

Although the Login preferences are not saved, user data is preserved through an upgrade (user ID and password). If user authentication was disabled prior to the upgrade, it will be enabled in the new software version. You will be required to enter a user ID and password when starting EncrypTight after the upgrade. Take one of the following actions to avoid being locked out of the application after upgrading to a new version of EncrypTight.

- Make sure that you know a valid EncrypTight administrator user name and password prior to upgrading.
- Delete all users prior to upgrading. The default user ID and password of admin/admin will remain as a valid account after all other users are deleted.

You can see existing accounts in the User Accounts editor (**Edit > User Accounts**). If you have any doubts about how to log in to an existing account, reset the administrator password.

Related topics:

- [“Managing EncrypTight Accounts” on page 65](#)
- [“Changing an EncrypTight User Password” on page 66](#)
- [“Using a Common Access Card” on page 294](#)

Managing EncrypTight Accounts

The EncrypTight administrator can manage user accounts as follows:

- Create new EncrypTight users
- Modify EncrypTight user names and passwords
- Delete EncrypTight user accounts

Table 16 EncrypTight user name and password conventions

Parameter	User Name	Password
Length	1-32 characters	1-256 characters
Case sensitive	Yes	Yes
Invalid characters	< > & “	< > & “
Spaces allowed	Yes	Yes
Must be unique	Yes	No
Other conventions	N/A	N/A

To add an EncryptTight user account:

- 1 From the Edit menu, click **User Accounts**.
- 2 In the User Accounts editor, click **Add**.
- 3 In the User dialog box, enter the user name, password, and select a group ID (admin or user). If Common Access Card Authentication is enabled, you also need to enter the common name from the user's certificate.
- 4 Click **OK**.

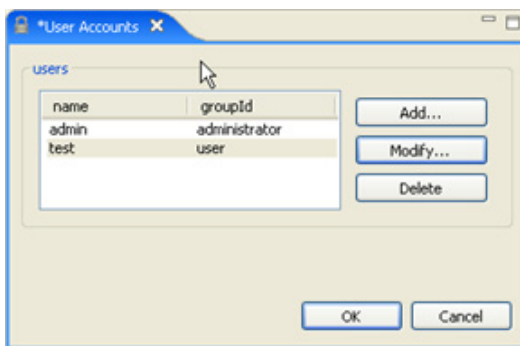
To modify an EncryptTight user account:

- 1 From the Edit menu, click **User Accounts**.
- 2 In the User Accounts editor, select a user from the list and click **Modify**.
- 3 Make the desired changes and click **OK**. Password changes takes effect immediately.

To delete an EncryptTight user account:

- 1 From the Edit menu, click **User Accounts**.
- 2 In the User Accounts editor, select a user from the list and click **Delete**.

Figure 17 Add, modify, and delete users in the User Accounts editor



Related topics:

- [“Configuring EncryptTight User Authentication” on page 62](#)
- [“Configuring the Password Enforcement Policy” on page 103](#)

Changing an EncryptTight User Password

Users and administrators can change their own passwords using the **Change User Password** option in the Edit menu. See [Table 16](#) for a summary of password conventions.

To change a password:

- 1 From the Edit menu, click **Change User Password**.
- 2 In the Change Password window, enter the current password. Then enter the new password and reenter to confirm.
- 3 Click **Apply**. The password change takes effect immediately.

How EncrypTight Users Work with ETEP Users

EncrypTight manages ETEP user accounts. In order for EncrypTight to communicate with the ETEP, it needs to know the ETEP's user name and password. It will try to use the credentials that you used to log in to EncrypTight. If that doesn't match the credentials that are configured on the ETEP, EncrypTight will ask you to enter the appliance user name and password. EncrypTight will remember these appliance credentials for the duration of the EncrypTight session.

To avoid having to enter the ETEP credentials each session, create an EncrypTight account with credentials that match the ETEP user accounts. Then log in to EncrypTight using the account that matches the ETEPs that you are managing.

Table 17 summarizes the relationship between EncrypTight users and ETEP users, which is explained in more detail in the examples that follow.

Table 17 Relationship between EncrypTight users and ETEP users

Situation	EncrypTight user ID and password	ETEP user ID and password	Result
Default users (“Example 1: Default EncrypTight user and default ETEP user”)	admin/admin	admin/admin	OK. EncrypTight can manage the ETEP.
Custom users (“Example 2: Setting up new EncrypTight and ETEP users”)	beacon/lighthouse	beacon/lighthouse	OK. EncrypTight can manage the ETEP.
Mismatched users (“Example 3: Adding a new ETEP user to EncrypTight”)	beacon/lighthouse	admin/admin	Failed communication. EncrypTight prompts you to enter the ETEP credentials so that it can manage the ETEP.

Example 1: Default EncrypTight user and default ETEP user

In a new installation of EncrypTight, the default user name and password is **admin/admin**. The default user name and password on the ETEP is also **admin/admin**.

Without any changes to EncrypTight user accounts or ETEP appliance users, EncrypTight is able to manage the ETEP using the default user names and passwords. Log in to EncrypTight as **admin/admin** and manage the ETEP.

Example 2: Setting up new EncrypTight and ETEP users

Set up new EncrypTight and ETEP user names and passwords as follows:

- 1 Log in to EncrypTight as **admin/admin**.
- 2 Add an EncrypTight administrator user to match the user name and password that you plan to set up on the ETEPs. In this example we plan to set up an ETEP admin account with the user name **beacon** and password **lighthouse**. The first step is add a new EncrypTight account for a user called **beacon**, with password **lighthouse** and group ID **admin**.

Do not delete the default EncrypTight account of **admin/admin** until you have set up the new user on the ETEP (step 4).

- 3 In EncryptTight, add a new ETEP appliance and refresh its status. Because EncryptTight and the ETEP are both using their default user names and passwords of **admin/admin**, EncryptTight can successfully contact the ETEP.
- 4 From EncryptTight, select the new ETEP and add a new appliance user with the name **beacon**, password **lighthouse**, and role **admin**.

The next time you start EncryptTight, log in with the User ID **beacon** to manage the new ETEPs.

Example 3: Adding a new ETEP user to EncryptTight

This example adds a new ETEP appliance to an existing version of EncryptTight. The EncryptTight user is logged in to EncryptTight with the user name **beacon** and password **lighthouse**. The new ETEP has its default user name and password of **admin/admin**.

- 1 Log in to EncryptTight as **beacon/lighthouse**.
- 2 In EncryptTight, add a new ETEP appliance and refresh its status.
- 3 When you refresh the status, EncryptTight notifies you that the EncryptTight credentials don't match those on the ETEP. To continue, enter the ETEP's default user name and password when prompted (**admin/admin**).



- 4 From EncryptTight, add the new user name **beacon** and password **lighthouse** to the ETEP (**Tools > Appliance Users > Add User**). The EncryptTight and ETEP accounts now match, allowing EncryptTight to communicate with the ETEP without requiring any additional verification.

Related topics:

- [“Working with EncryptTight User Accounts” on page 61](#)
- [“Appliance User Management” on page 102](#)

5 Maintenance Tasks

This section includes the following topics:

- [Working with the EncrypTight Workspace](#)
- [Installing Software Updates](#)
- [Upgrading External ETKMSs](#)

Working with the EncrypTight Workspace

The EncrypTight workspace contains all the elements that EncrypTight is managing, such as appliance configurations, data associated with ETPM and certificate information. The following topics describe how the EncrypTight workspace is structured, and how it is used to store workspace contents:

- [“About the EncrypTight Workspace” on page 69](#)
- [“Saving a Workspace to a New Location” on page 70](#)
- [“Loading an Existing Workspace” on page 71](#)
- [“Moving a Workspace to a New PC” on page 72](#)
- [“Deleting a Workspace” on page 72](#)

About the EncrypTight Workspace

The workspace directory contains directories for appliances, factory configurations, defaults, and policy templates. Data generated by ETPM is also stored in the workspace directory. Note that no ETPM data is saved until you add at least one PEP in the ETEMS Appliance Manager.

EncrypTight considers the most recently opened workspace to be the active one. The file name and path are displayed in the application’s title bar. New and changed appliance configurations are saved to the active workspace.

By default the configuration files are stored in <InstallDIR>\data, where InstallDIR is the top-level EncrypTight directory. You can store your workspace in the default directory or choose one of your own.

**CAUTION**

Appliance configurations and policy files are stored as .xml files. These files are not encrypted or password protected. They can be opened and edited using a basic text editor. Take precautions to protect these files from unauthorized access.

EncrypTight allows you to save more than one workspace. This can be useful for backup purposes, or to segregate your work in a complex deployment. Although the EncrypTight workspace is opened and saved using the management workstation's file system, individual appliances and policies should be added and deleted only in the EncrypTight application.

Related topics:

- [“Saving a Workspace to a New Location” on page 70](#)
- [“Loading an Existing Workspace” on page 71](#)
- [“Moving a Workspace to a New PC” on page 72](#)

Saving a Workspace to a New Location

The following items are saved in a workspace:

- The EncrypTight license (EncrypTight software version 1.9 and later)
- Appliance configurations
- Data that pertains to ETPM

Factory configurations and customized default configurations are considered global settings, and therefore are not saved with a workspace. The most recently defined default configuration for each appliance model/software combination is considered the active one, and is applied across workspaces.

When you save a workspace to a new location, the original workspace remains active. To make the backup workspace the active one, you need to explicitly load it (see [“Loading an Existing Workspace” on page 71](#)). To verify which workspace is active, check the directory path in the title bar.

To save a workspace to a new location:

- 1 On the **File** menu, click **Save Workspace To**.
- 2 Select a location for the saved workspace, using one of the methods listed below.
 - To create a new directory, navigate to the location of the new directory and click **New Folder**. Highlight the New Folder and rename it, and then click **OK**. This creates a duplicate workspace. The new folder can be located anywhere *except* under the EncrypTight home directory.
 - To select an existing directory in which to save the appliance configurations, locate the directory and select it. Click **OK**. This adds new appliances to an existing workspace.

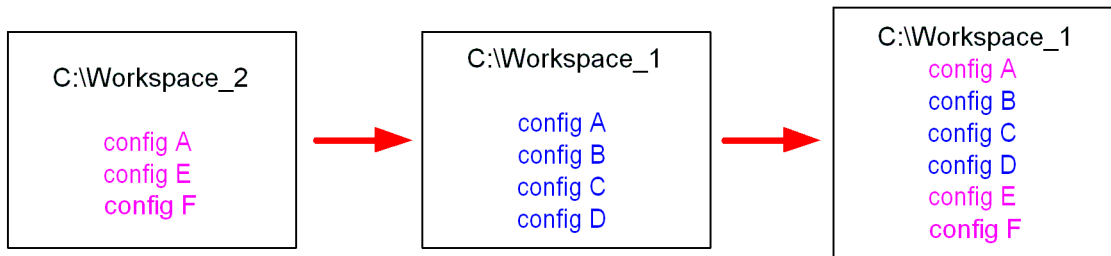
If you save the current workspace to a directory that contains a pre-existing workspace, be aware of duplicate appliance names. If any of the appliance names are duplicated, the new appliance configuration in the current workspace will overwrite the configuration of that appliance in the pre-existing directory. In [Figure 18](#), when Workspace_2 is saved to Workspace_1, Configuration A from Workspace_2 overwrites Configuration A in Workspace_1. Configs E and F are added to Workspace_1.

Figure 18 Saving one workspace to another

Workspace_2 (WS_2) is the open workspace. WS_1 is the target directory.

When WS_2 is saved to WS_1...

...WS_2 config A overwrites WS_1 config A. WS_1 becomes the open workspace.



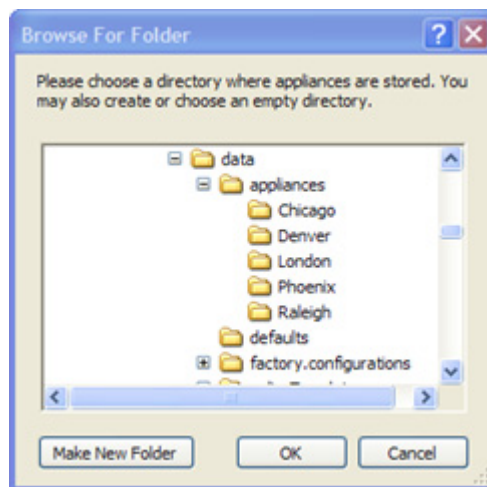
Loading an Existing Workspace

Reasons for loading an existing workspace are:

- To load a saved workspace on a new management station
- To restore a backup copy if the active workspace is damaged
- To revert to previous appliance configurations and policies
- To work on a different group of appliances in a network that has been segmented into several workspaces.

To load an existing workspace:


- 1 On the **File** menu, click **Load Workspace**.



- 2 Browse for the location of the saved workspace and click the directory name to select it.

Be sure to select the top level workspace directory and not the directory of an individual appliance or subdirectory within the group. In the figure above, the workspace name is `data`. The `data` directory contains a subdirectory named `appliances` with appliance configurations named `Chicago`, `Denver`, `London`, `Phoenix`, and `Raleigh`. The `data` directory also contains directories named `defaults`, `factory.configurations`, and `policyTemplates`.

- 3 Click **OK**. The new workspace is loaded, replacing the previously active workspace. The appliances' status appears as **?**.

- 4 Refresh the appliances' status. From the **Edit** menu click **Select All**, then click .

Related topic:

[“Moving a Workspace to a New PC” on page 72](#)

Moving a Workspace to a New PC

To transfer your workspace to a new management PC, save the `data` folder to an interim location and then load it into the application on the new PC.

To move a workspace to a new PC:

- 1 On the old PC, click **File > Save Workspace To** and browse to an interim storage location such as a network drive or USB drive. Click **OK** to save a copy of the `data` folder.
- 2 Install the EncrypTight software on the new PC and start the application.
- 3 In the Appliance Manager, click **File > Load Workspace** to load the `data` folder from the interim storage device into ETEMS. When prompted by Windows Explorer, browse to the location of the saved `data` folder, select it, and click **OK**.

The workspace is loaded into EncrypTight. However, EncrypTight assumes that the interim storage location is the active workspace.

- 4 To copy the workspace from the interim storage device to the new PC, click **File > Save Workspace To**. Browse to the top level EncrypTight installation directory, typically `\Program Files\EncrypTight`. Select the `EncrypTight` directory and click **OK** to copy the `data` folder to it.
- 5 To change the location of the active workspace from the interim storage device to the EncrypTight installation directory, click **File > Load Workspace**, browse to the location you selected in the previous step, and click **OK**.

 **NOTE**

EncrypTight 1.9 and later is a licensed product. Because EncrypTight licenses are specific to the computer on which they are installed, you will need to acquire and install a new EncrypTight license for the new computer. Contact Customer Support to acquire a new license key (see [“Contacting Black Box Technical Support” on page 14](#)).

Related topics:

- [“Saving a Workspace to a New Location” on page 70](#)
- [“Loading an Existing Workspace” on page 71](#)

Deleting a Workspace

Workspaces are deleted in the same way that you delete any other folder or directory on your PC. The only time that you should use your PC's file system to manipulate EncrypTight files is to delete *workspaces*. Use EncrypTight to delete individual appliances and policies from a workspace.

To delete a workspace:

- 1 On your PC's hard drive, locate the workspace that you want to delete.
- 2 Delete the workspace directory.

Installing Software Updates

Software updates for EncrypTight are available separately from the PEP software. You might need to update all of the components in your system, or only specific components. This procedure assumes that you are updating all of the components of EncrypTight. If you are upgrading from software versions that are several years old, contact customer support for assistance with your upgrade path.

To upgrade EncrypTight to a new release, take the following steps:

- [Step 1: Schedule the Upgrade](#)
- [Step 2: Prepare ETPM Status and Renew Keys](#)
- [Step 3: Upgrade the EncrypTight Software](#)
- [Step 4: Verify ETKMS Status and Deploy Policies](#)
- [Step 5: Upgrade PEP Software](#)
- [Step 6: Change the PEP Software Version and Check Status](#)
- [Step 7: Return Status Refresh and Key Renewal to Original Settings](#)

Step 1: Schedule the Upgrade

Proper scheduling of your upgrade is imperative to minimize traffic disruptions. ETKMSs communicate with PEPs to deploy policies, and to renew keys and refresh policy lifetimes. The upgrade process for the ETKMSs and the EncrypTight software can interrupt this communication, and the upgrade for a PEP interrupts data traffic when the PEP reboots.

Review the following guidelines prior to scheduling an upgrade:

- Schedule the upgrade during a planned and approved maintenance window
- Do not deploy policies during the upgrade process
- Do not perform upgrades when keys are scheduled to be renewed.

To prevent key renewal during the upgrade process, check the **Renew Keys/Refresh Lifetime** setting on each policy defined in ETPM. There are two types of settings: daily at a specific time and periodically at an interval between 0 to 65535 hours.

- For policies that renew and refresh at a specific time of day, find a period when there is enough time to complete the upgrade before the scheduled key renewal.
- For policies that renew periodically, temporarily change these policies to provide enough time to complete the upgrade. Consider using zero lifetime policies, which don't rekey, until the upgrade process is complete.

The upgrade process should take about 30 minutes for each external ETKMS, 15 minutes for the EncrypTight software, and 5-15 minutes for each PEP. You can upgrade multiple PEPs at the same time, which can shorten the total length of time it takes to perform the full upgrade process.

Once you start, the ETKMSs and the EncrypTight software must be upgraded in sequence. After these upgrades are complete, you need to deploy your policies in order to trigger the ETKMSs to generate a new policy database. You should take this step before you upgrade the PEPs. Because this will interrupt traffic on the PEPs briefly, you should consider the timing of this step as you plan your upgrade.

After these upgrades are complete, you can upgrade the PEPs.

You can schedule the upgrade for each PEP at different time, depending on the rekey settings and data traffic requirements. Because a reboot is required, the upgrade of each PEP interrupts traffic through that PEP for several minutes.

Step 2: Prepare ETPM Status and Renew Keys

To prepare ETPM status and renew keys:

- 1 To ensure that status information is not communicated during the upgrade, disable the ETPM automatic status refresh.
 - a From the ETPM main menu bar, click **Edit > Preferences**.
 - b In the Preferences window, expand the ETPM listing and select **Status**.
 - c Note the current status settings and then disable the automatic status refresh.
- 2 To initialize the key interval settings and allocate the longest possible time for the upgrade, manually renew the keys. From the ETPM main menu bar, click **Tools > Renew Keys**.

Step 3: Upgrade the EncrypTight Software

EncrypTight has a combined software installation that includes ETEMS, ETPM, and local software ETKMS.

To upgrade to the new version of EncrypTight:


- 1 If you use a local ETKMS, stop it before you proceed. To stop the local ETKMS, display the ETKMS window and press CTRL + C, or close the window. For more information, see [“Launching and Stopping a Local ETKMS” on page 45](#).
- 2 Uninstall the old version of EncrypTight or ETEMS.
 - a In the Microsoft Windows Control Panel, click **Add or Remove Programs**.
 - b From the list of programs, select the program to uninstall (EncrypTight). Click **Change/Remove**.
 - c The uninstall wizard asks if you want to save the appliance configurations. Click **Yes** to save the configurations for use in the new version. This saves your appliance configurations, policies, and default configurations. It also saves your current EncrypTight license (software version 1.9 and later). If you do not choose to save, you will need to reinstall the EncrypTight license.
- 3 Install the new version of EncrypTight. Insert the EncrypTight CD into the management station’s CD-ROM drive and follow the instructions in the installation wizard. If the installation program does not start automatically, open the CD and double-click `EncrypTight.exe`.

Step 4: Verify ETKMS Status and Deploy Policies

After EncrypTight is upgraded, check the status of the ETKMSs and deploy the policies.

To check the ETKMS status:

- 1 From ETEMS, select all ETKMSs and select **Tools > Refresh**.

All ETKMSs should return a  status.

To deploy policies:

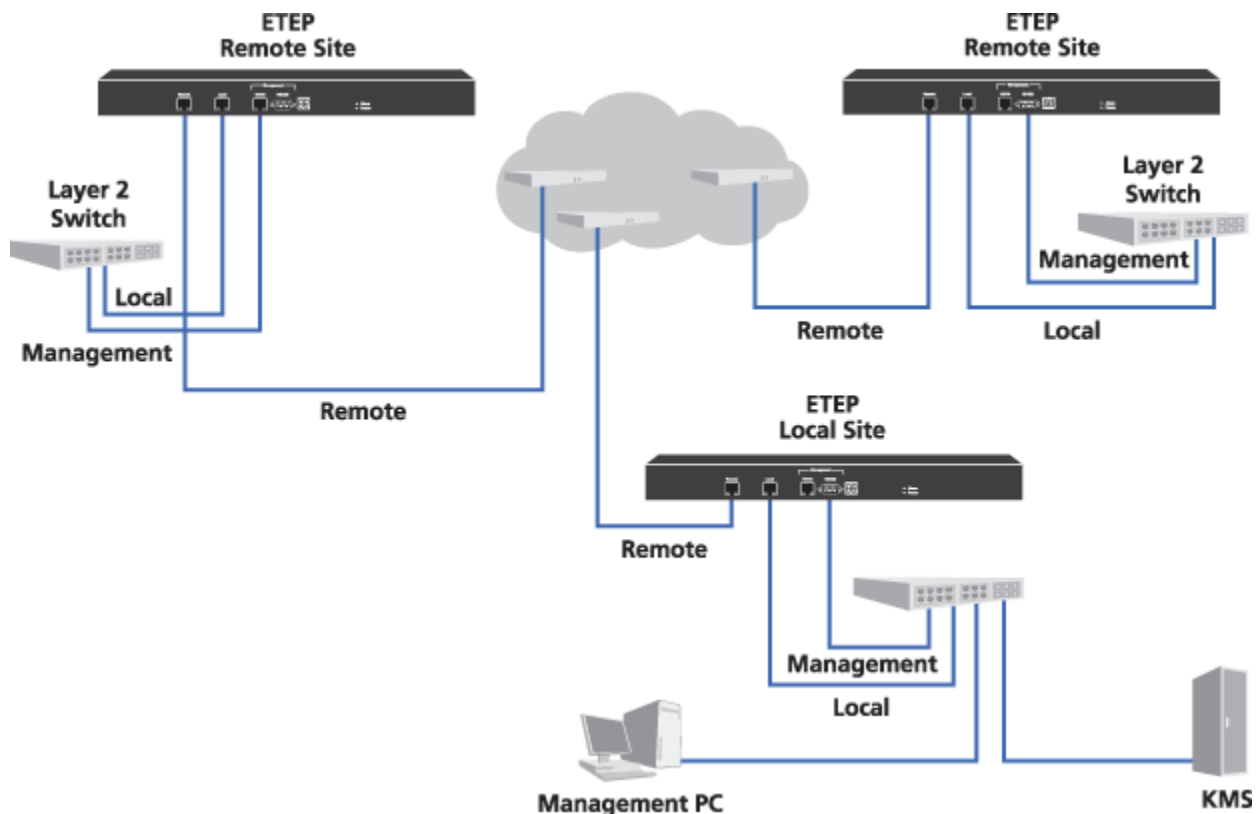
- 1 Click **Tools > Deploy** to synchronize the EncrypTight components with the current policies. Note that this will interrupt traffic on the PEP briefly.

Step 5: Upgrade PEP Software

After you upgrade the ETKMSs and ETPM, you can upgrade the PEPs to a new software version. Using ETEMS, you can download new software from an FTP server to one or many PEPs of the same product family. For example, ETEMS can upgrade a mix of ETEP models, such as ET0010As, ET0100As, and ET1000As, in a single operation.

When upgrading software on ETEP 1.6 and later appliances, you have the option of using FTP or SFTP for secure file transfer. If you choose SFTP as the connection method, all of the selected appliances must support SFTP.

Figure 19 Upgrade remote appliances first when managing appliances in-line, where management traffic flows through the data path



If you are managing your PEPs in-line as shown in [Figure 19](#), we recommend performing a software upgrade in two stages. First, upgrade all the PEPs at remote sites and reboot them. When the remote site PEPs are up and operational, upgrade the local site PEP, which is co-located with the EncrypTight management station. Upgrading the local site PEP at the same time as the remote PEPs can cause connectivity with the management station to be lost and the remote site upgrades to fail.

**CAUTION**

Software upgrades require a reboot to take effect. Rebooting the PEP interrupts data traffic for approximately two minutes. During this time all packets are discarded.

To upgrade software on the PEPs:

- 1 From the EncryptTight Enforcement Point CD for the PEPs that you want to upgrade, copy the folder for your appliance model to your default FTP directory.
For example, if you are upgrading ETEP PEPs, copy the ETEP folder to your FTP directory.
- 2 In the Appliance Manager, select the PEPs to upgrade. If you are managing the PEPs in-line, upgrade the remote site PEPs first before upgrading the data center PEP, as shown in [Figure 19](#).
- 3 On the **Tools** menu, click **Upgrade Software**.
- 4 Enter the **FTP server site** information for the upgrade software, as described in [Table 18](#). Do not use the following special characters in the FTP user name and password: @ : ? # < > &.
Optional. Click **Verify** to confirm that the site is reachable. If it is not, ETEMS displays a message indicating the nature of the problem.
ETEP PEPs automatically back up the file system prior to upgrading. If you experience a problem with an upgrade, you can then restore the PEP's file system from the backup copy.
- 5 Select the **Reboot after upgrade** check box to automatically reboot the PEPs immediately following a successful upgrade. To reboot at a later time, clear the check box.
- 6 Click **Upgrade**. Upgrade results for each appliance are displayed in the Result column of the Upgrade Appliances table.
- 7 Upgrading the software version on the appliance does not automatically update the ETEMS configuration. After the appliances have been rebooted, you can edit the ETEMS configurations to reflect the new software version running on the appliances (**Edit > Multiple Configurations > Software Version**).

Table 18 FTP server site information for appliance software upgrades

Field	Description
Host	IP address of the management workstation running the FTP server software. If you are retrieving log files from a host that has already been configured, you can select its IP address from the Host box. ETEMS completes the remaining FTP server information for you based on the selected host IP address. ETEP 1.6 and later appliances support IPv4 and IPv6 addresses. If you are using an IPv6 host address, all of the selected appliances must support IPv6.
Path	The directory on the FTP server that contains the files of interest. Valid entries are the default FTP directory and its subdirectories. Enter the directory listing relative to the default directory. If the files are located in the default directory, leave this field blank.
User	User ID of a user on the FTP server. Do not use the following characters: @ : ? # < > &
Password	Password associated with the user name. Do not use the following characters: @ : ? # < > &
Connection Method	FTP is the default file transfer protocol and is supported on all appliance models and software revisions. SFTP provides secure file transfer. It is supported on ETEP appliances running version 1.6 and later software.

 **NOTE**

- *You must reboot the ETEP PEPs after you upgrade. If you make any configuration changes to the ETEP PEPs after you upgrade and before you reboot, those changes will be lost when the PEP reboots.*
- *If you decide later to undo the upgrade and restore a previous file system to the PEPs, you could inadvertently restore expired policies and out of date keys. You should redeploy your policies from ETPM to make sure that all of your PEPs have current policies and keys.*


Step 6: Change the PEP Software Version and Check Status

To enable access to any new features available with the upgrade and avoid inconsistent status indicators, you must change the software version in the Appliance Manager for each of your PEPs. In order to check for the correct operation and connectivity of all EncrypTight components, check the status of the PEPs and policies.


To change the software version of the PEPs:

- 1 In the Appliance Manager, select the target appliances in the Appliances view. The selected appliances must all be the same hardware model, for example ET0100A.
- 2 Click **Edit > Multiple Configurations > Software Version**.
- 3 In the Modify Software Version window, select the software version from the list and then click **Apply**.
- 4 From the Appliances view, select the target appliances and push the new configuration to the appliances (**Tools > Put Configuration**).

To check the status of the PEPs:

- 1 In the Appliance Manager, highlight all PEPs and select **Tools > Refresh**.
All PEPs should return a  status. If you see other status indicators, refer to [Chapter 18](#) for troubleshooting information to help resolve the issues.

To check the policy status:

- 1 From ETPM, click **Deploy Policies**.
All policies should return a  status. If you see other status indicators, refer to [Chapter 18](#) for troubleshooting information to help resolve the issues.

Step 7: Return Status Refresh and Key Renewal to Original Settings

To return status refresh and key renewal to their original settings:

- 1 If you disabled the automatic status refresh in ETPM in “[Step 2: Prepare ETPM Status and Renew Keys](#)” on page 74, select **Edit > Preferences** and select **ETPM Status**. Click the **Enable automatic status refresh** check box and set the **Refresh interval (in minutes)**.
- 2 If you changed the Renew keys/Refresh lifetime setting for any policies, edit each policy to reset the **Renew keys/Refresh lifetime** to the previous value and deploy the modified policies (**Tools > Deploy**).

Upgrading External ETKMSs

Local ETKMSs are upgraded when you install a new version of the EncrypTight software. See “[Step 3: Upgrade the EncrypTight Software](#)” on page 74 for the local ETKMS upgrade procedure. The following information is provided in the event that you need to upgrade the software for external ETKMSs.

Because you might need to restore some settings after the upgrade, record the following:

- The IP address and name of the ETKMS in the `/opt/etkms/bin/etkmsParams.sh` file.
- Any custom settings you made in the `/opt/etkms/conf/kdist.properties` file.

If you use backup ETKMSs, upgrade the primary and backup ETKMSs at the same time.

The general steps to upgrade a ETKMS are:

- 1 Stop and remove the current ETKMS software.
- 2 Install the new ETKMS software.
- 3 Configure the new software.
- 4 Start the ETKMS software.

To stop and remove the current ETKMS software:

- 1 Login as the root user.
- 2 Type the following to stop the ETKMS service:

```
service etkms stop
```

If you use a backup ETKMS, stop the backup ETKMS first and then stop the primary ETKMS service.

- 3 Type the following to uninstall the ETKMS software:

```
rpm -e etkms
```

The `rpm -e` command moves the old ETKMS software to the `/opt/etkms.backup` file. This includes the `bin/etkms.params.sh` file, the `conf/kdist.properties` file, and the `keys/` directory.

- 4 Type the following to move the `etkms.backup` directory to `etkms.orig` (in case you need to restore the original software later):

```
mv /opt/etkms.backup /opt/etkms.orig
```

To mount the CDROM drive:

- 1 Insert the disk in the drive and close it.
- 2 If it doesn't already exist, create the directory `/media/cdrom`.

```
mkdir /media/cdrom
```

- 3 Enter the following command:

```
mount -t iso9660 /dev/scd0 /media/cdrom
```

To install the new ETKMS software:

- 1 Install ETKMS RPM with the following commands:

```
cd /media/cdrom
```

```
rpm -ivh etkms.rpm
```

- 2 Verify that the ETKMS RPM is installed and unmount the CD with the following commands:

```
rpm -qi etkms
```

```
cd /
```

```
umount /media/cdrom
```

```
eject
```

To configure the new ETKMS software:

- 1 Edit `/opt/etkms/bin/etkmsParams.sh` for the correct IP address and ETKMS name.
- 2 Edit `/opt/etkms/conf/kdist.properties` for any custom settings.

**NOTE**

If you have custom certificates installed, use the following command to copy the `etkms.keystore` file from `etkms.orig` directory to the `/keys` directory.

```
cp /opt/etkms.orig/keys/etkms.keystore /opt/etkms/keys/etkms.keystore
```

To start the ETKMS software:

- 1 Type the following to start the ETKMS service.

```
service etkms start
```

If you use a backup ETKMS, start the primary ETKMS first and then start the backup ETKMS.

**TIP**

To verify that the ETKMS is running, type:

```
service etkms status
```


Part II Working with Appliances using EEMS



6 Getting Started with ETEMS

This section includes the following topics:

- [ETEMS Quick Tour](#)
- [Understanding the ETEMS Workbench](#)
- [Understanding Roles](#)
- [Modifying Communication Preferences](#)

ETEMS Quick Tour

ETEMS is the appliance management feature of EncrypTight. ETEMS provides the ability to provision and manage multiple EncrypTight appliances from a central location. The primary tasks that ETEMS supports are:

- [“Defining Appliance Configurations” on page 83](#)
- [“Pushing Configurations to Appliances” on page 84](#)
- [“Upgrading Appliance Software” on page 85](#)
- [“Comparing Configurations” on page 85](#)
- [“Maintenance and Troubleshooting” on page 86](#)
- [“Policy and Certificate Support” on page 87](#)

Defining Appliance Configurations

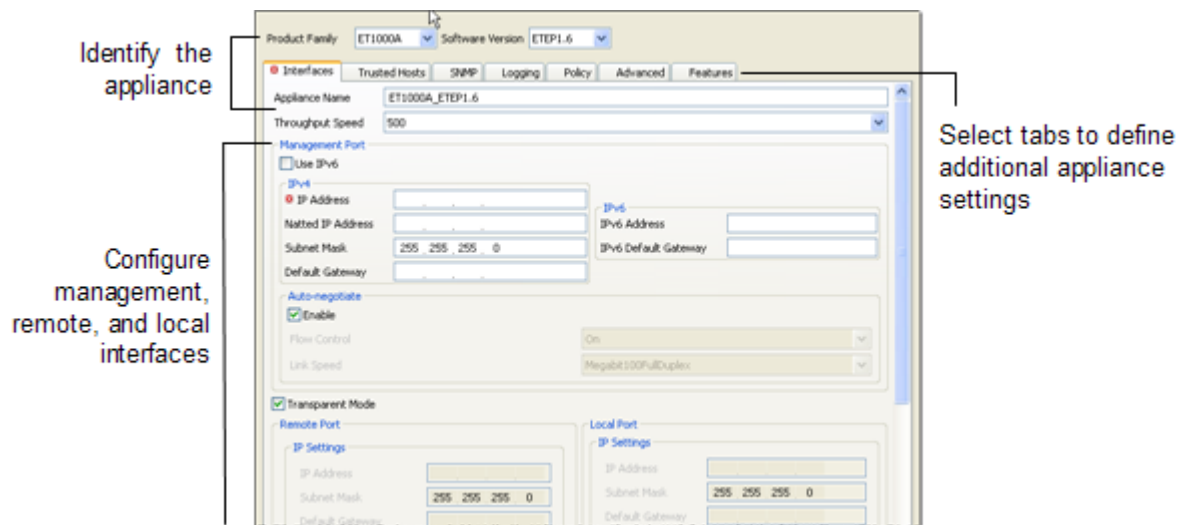
When configuring a new appliance (**File > New Appliance**), the first thing to do is select the product family and software version. ETEMS displays a configuration screen tailored to the specified appliance model and software version. On most appliance models the **Interfaces** tab contains the fields required to identify an appliance: its name, password access to the appliance, and the interface IP addresses.

Select other tabs to configure additional items on the appliance, such as EncrypTight features, SNMP or logging. The availability of specific tabs and configuration options varies depending on your appliance model and software version.

Most of the information contained on the additional tabs will be the same for all of the appliances of a particular model that you configure. To streamline the configuration of a large number of appliances, use

the factory default configurations or define your own template for these common values (**Edit > Default Configurations**).

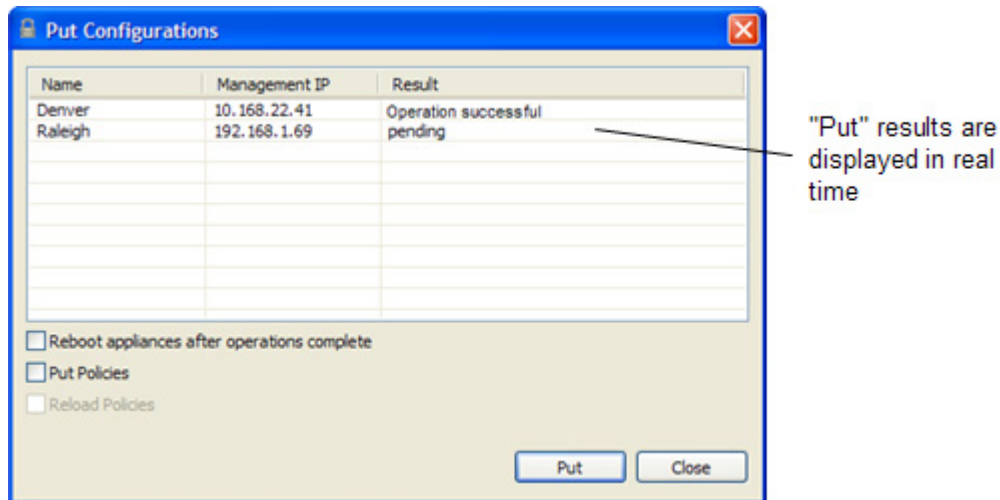
Figure 20 Interface configuration for a new ET1000A appliance



Pushing Configurations to Appliances

Use the Put Configurations window to push the configurations defined in ETEMS to the appliances. In the Appliance Manager, select the target appliances in the Appliances view. Then in the Tools menu, choose **Put Configurations**. During the “put” operation, when ETEMS pushes the configurations to the appliances, ETEMS displays the status of the operation.

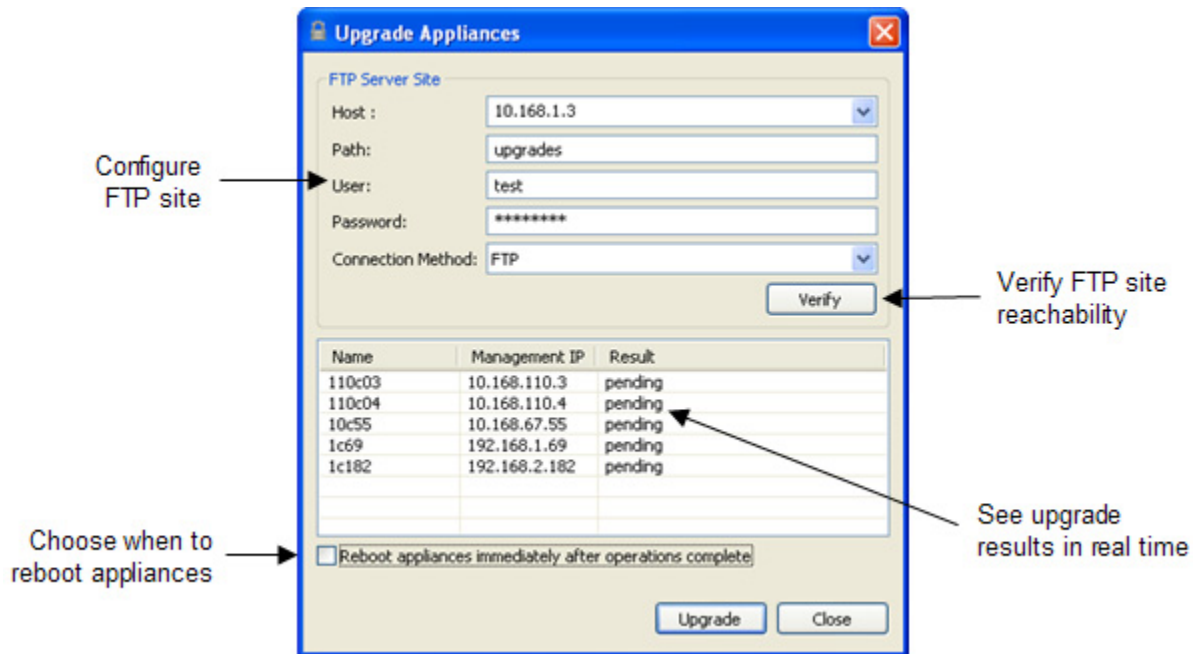
Figure 21 Status is shown for each target appliance when configurations are pushed



Upgrading Appliance Software

New revisions of appliance software can be loaded on the appliances from an FTP server. Simply copy the new software to an FTP server, select the target appliances, and point to the FTP server site. Results for each appliance are displayed as they are upgraded. The new software takes effect upon appliance reboot.

Figure 22 Upgrade software on appliances from a central location



Comparing Configurations

The Compare Config to Appliance feature on the Tools menu displays the configuration stored in ETEMS and the configuration running on the appliance. If the configurations differ, this feature can help you discover and resolve discrepancies. A green check mark indicates that ETEMS and appliance settings are the same. If the settings are unequal, you can synchronize them by copying appliance settings to ETEMS or pushing the ETEMS configuration to the appliance.

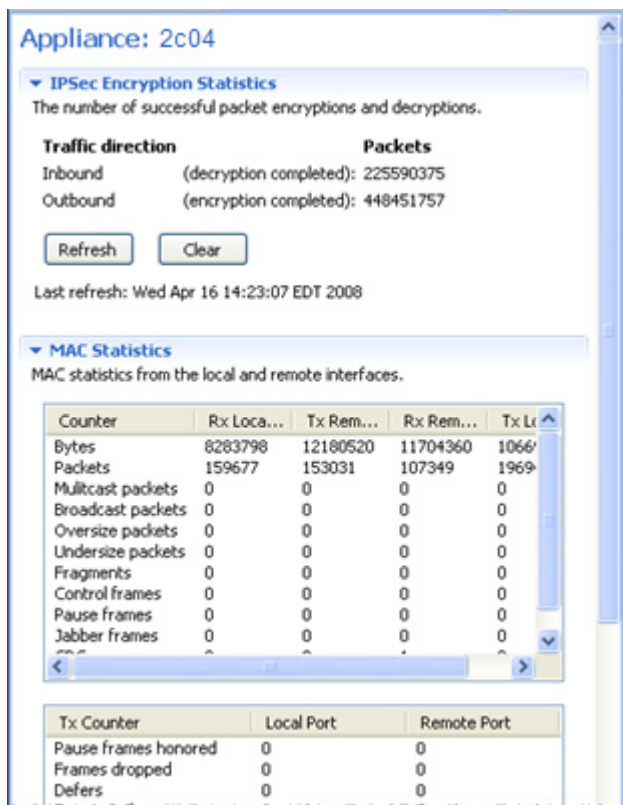
Figure 23 Compare the ETEMS configuration to the appliance to discover discrepancies

Property	ETEMS Configuration	Appliance Configuration
Log Facility Priority:Local2	warning	info
Management Interface: Truste...	TrustedHostEntry {□□Applanc...	TrustedHostEntry {□□}
SNTP Client: Enable	true	false
SNTP Client: NTP Service IP Ad...	10.168.1.8	0.0.0.0
Syslog Servers	SyslogServers {□□ApplianceCo...	SyslogServers {□□}
Appliance Group Id	0	0
Appliance IKE VLAN Tag Enabled	false	✓ false
Appliance IKE VLAN Tag Identi...	1	✓ 1
Appliance IKE VLAN Tag Priority	0	✓ 0
Appliance Policy Ike Authentic...	PresharedKey	✓ PresharedKey
Appliance Policy Preshared Key	01234567	✓ 01234567
Appliance Policy Traffic	EthEncrypt	✓ EthEncrypt
Appliance Role	Primary	✓ Primary
Appliance Setting CLI: Session ...	10	✓ 10
Appliance Setting FIPS Enabled	false	✓ false
Appliance Setting Non IP Traffi...	Clear	✓ Clear

Maintenance and Troubleshooting

ETEMS includes tools for monitoring and maintaining EncrypTight appliances. Some of ETEMS's capabilities include:

- Retrieving appliance log files
- Displaying performance and diagnostic statistics ([Figure 24](#))
- Accessing the appliance CLI to perform administrative tasks and issue diagnostic commands.

Figure 24 Statistics view displays a snapshot of performance data on the ET0100A

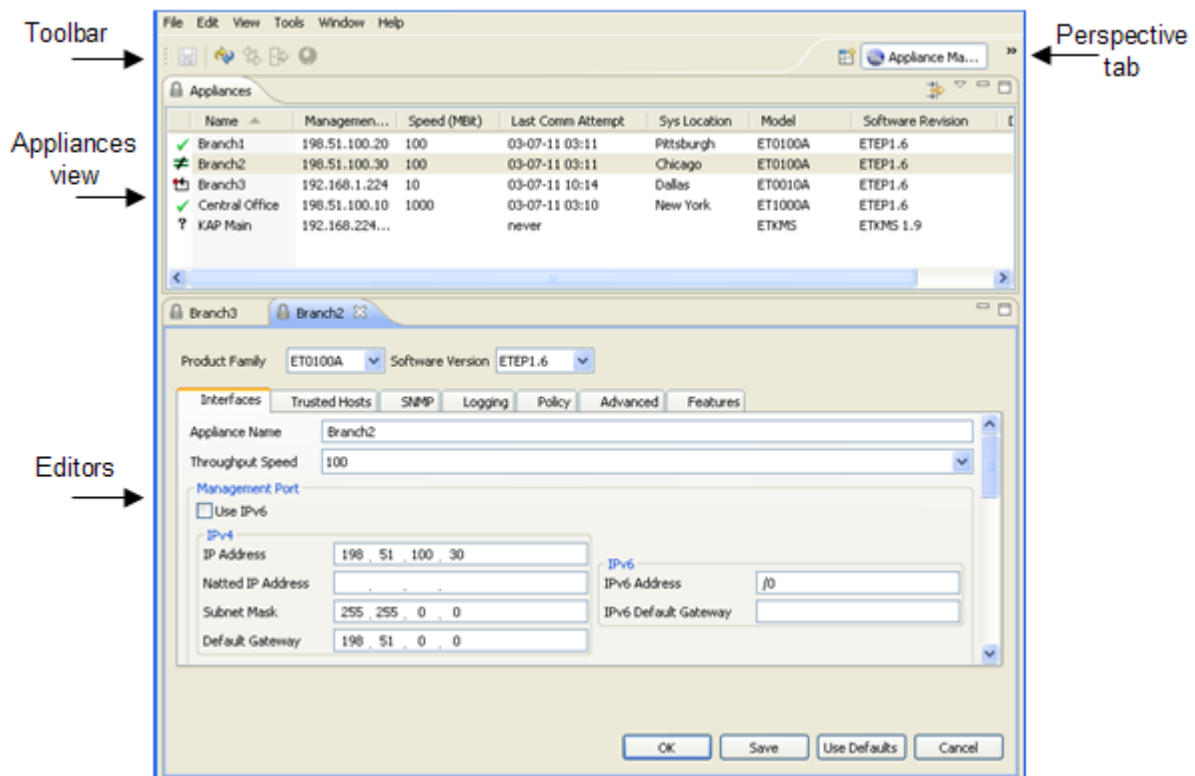
Policy and Certificate Support

ETEMS's policy feature is limited to the creation of point-to-point policies. For larger, more complex deployments use the Management and Policy Server (ETPM) to create, manage and deploy distributed key policies.

ETEMS's policy and certificate management capabilities vary by appliance model. On some models point-to-point policy and certificate management is available directly in ETEMS; other models support these functions only from the appliance's web interface. See the configuration chapter for your appliance model for details about specific features and functions.

Understanding the ETEMS Workbench

The ETEMS workbench contains all the elements that ETEMS is managing, such as appliance configurations, policy information, and any data associated with ETEMS perspectives, which are essentially task-specific features. This section explains the main sections of the workbench and how to navigate among them.

Figure 25 Appliance Manager perspective

Views

Views display information about items that ETEMS manages, such as appliance configurations or certificates. When you start ETEMS, the Appliance Manager opens and displays the Appliances view. Initially the Appliances view is empty. After you add appliances to ETEMS, the appliances appear in the view along with their operational status, IP addresses, product family and software version, the timestamp of when ETEMS last communicated with the appliance, and the appliance's date and time.

From the Appliances view you can select appliances to edit, delete, or upgrade with a new version of software. Sort appliances by clicking the table column headers. Click and drag the Appliances tab to reposition the Appliances view around the editor. To focus on a specific subset of appliances, you can filter them based on management IP address.

Some ETEMS actions can be applied to a group of target appliances:

- To select a contiguous block of appliances, click the first appliance to select it. Then press and hold the Shift key and click the last appliance in the block.
- To select several non-contiguous appliances, click the first appliance to select it. Then press and hold the CTRL key while selecting the other appliances.

Editors

Editors in ETEMS allow you to add and change configuration information. Each editor is task-specific, such as an appliance configuration editor or a policy editor. You can arrange the views and editors to suit your needs, as described below.


- You can open multiple appliance editors at the same time. The editors are stacked in a tabbed panel. Tabbed editor windows allow you to work on more than one appliance or switch to editors from add-on features.
- Editors can be stacked on top of other editors or positioned left to right. When multiple appliance editors are open, you can drag one editor next to another for a side-by-side or top-to-bottom comparison.
- Click and drag a view or editor tab to move it. Or, right-click a view or editor tab to move, size, maximize or minimize the view or editor. You can also maximize views and editors by double-clicking their tabs. Double-clicking a tab again restores the previous layout.
- File menu options allow you to save, save all, close, or close all open editors.

Perspectives

Perspectives show the functionality associated with a task, such as appliance configuration, certificate management, or policy management. Each perspective has its own unique set of editors, views, and toolbars that are relevant to its task. Only one perspective is visible at any time. ETEMS includes the following perspectives:

- Appliance Manager is a tool for defining appliance configurations, pushing configurations to appliances, comparing configurations, and upgrading appliance software.
- Certificate Manager is a tool for managing certificates on appliances, including generating certificate requests and installing certificates.
- Policy Manager (ETPM) is a tool for creating and distributing security policies and encryption keys.

To open a perspective:

- 1 There are two ways to open a perspective. Do one of the following:
 - In the Window menu, click **Open**. Select a perspective from the list or click **Other** for a complete list of perspectives, including those installed as plug-ins.
 - On the Perspective tab in the upper right corner of the screen, click the Open Perspective button . Select a perspective from the list or click **Other** for a complete list of perspectives.

Related topics:

- [“Toolbars” on page 89](#)
- [“Status Indicators” on page 90](#)

Toolbars

The ETEMS toolbar provides shortcuts to frequently performed tasks.

Table 19 ETEMS toolbar










Button	Description
	Save appliance configuration.
	Refresh appliance status.
	Compare ETEMS and appliance configurations.
	Push ETEMS configurations to appliances.

Table 19 ETEMS toolbar

Button	Description
	Launch the web interface for an appliance.





The Appliance Manager has its own toolbar that lets you minimize and maximize the view, and filter the appliances that are displayed.

Table 20 Appliance Manager toolbar

Button	Description
	Filter appliances based on management IP address. Only those matching the filter pattern are shown in the Appliances view.
	Display the menu of Appliance toolbar actions. This provides an alternate method of displaying the Filter Appliances dialog box.
	Minimize the Appliances view.
	Maximize the Appliances view.

The Certificate Manager toolbar has buttons for generating, installing, and managing certificates. Mouse over each button to see a tooltip indicating its function.

Table 21 Certificate Manager toolbar

Button	Description
	<ul style="list-style-type: none"> View certificates View CRLs
	View certificate signing requests.
	Generate certificate signing request.
	<ul style="list-style-type: none"> Install external certificate Install signed certificate Install CRL

Status Indicators

The Appliances view displays the appliances that are being managed by ETEMS and their operational status. To get the current status of the appliances, refresh the view. You can sort the status column to display all devices that are in an error state at the top of the list.

Table 22 Appliance status indicators








Status Indicator	Description
	Unequal configurations. The ETEMS and appliance configurations are different.
	OK. The ETEMS and appliance configurations are the same, and the appliance is reachable.

Table 22 Appliance status indicators

Status Indicator	Description
	Appliance reboot required.
	Reload policies required.
	Status unknown. The appliance is not responding to ETEMS's attempts to communicate with it or ETEMS hasn't yet queried the appliance status.
	Appliance unmanageable due to an incompatible hardware/software combination or runtime exception error.
	The appliance is in an error state.

Understanding Roles

EncrypTight and the EncrypTight appliances each have unique roles that control different aspects of the product. The following sections describe the roles and how they differ:

- [“EncrypTight User Types” on page 91](#)
- [“ETEP Appliance Roles” on page 91](#)

EncrypTight User Types

EncrypTight has two user types: administrator and user. The EncrypTight administrator controls access to the EncrypTight application; it does not control access to the EncrypTight appliances. The EncrypTight administrator can create, modify, and delete other users and passwords, while the user can change only its own password.

Related topics:

- [“Managing EncrypTight Users” on page 61](#)
- [“ETEP Appliance Roles” on page 91](#)

ETEP Appliance Roles

Roles on the appliance are associated with a set of privileges and tasks that a user is able to perform on the appliance, such as assigning passwords, defining configuration settings, or creating policies.

User management is performed using ETEMS or the CLI commands. Roles can be associated with specific user names and passwords. This allows the ETEP to track which user performed an action on the appliance as opposed to simply the role that performed the action. Each role can be associated with more than one user name.

ETEPs have two roles: Administrator and Ops.

- The Administrator has access to all of the appliance functionality. This includes assigning roles, user names and passwords to all appliance users, defining appliance configurations, and defining and

deploying policies. ETEMS uses the Administrator user to log in to the appliance. The Administrator also has access to all of the CLI commands.

- The Ops user logs in to the appliance only through the CLI and has access to a subset of the CLI commands.

Table 23 Appliance roles for ETEPs

Function	Administrator	Ops
Manage passwords and users	Yes, in ETEMS	No
ETEMS access	Yes	No
CLI access	Yes	Yes (subset of commands)

To learn more about using ETEMS for ETEP user management, see [“Appliance User Management”](#) on page 102.

Modifying Communication Preferences

ETEMS communication preferences pertain to the communication between ETEMS and an appliance. Communication preferences fall into two categories.

- General communications between ETEMS and the appliances ([Table 24](#)).
- Preferences that apply only when using strict authentication for EncrypTight components ([Table 25](#)). When strict authentication is enabled, all TLS communications between EncrypTight components is authenticated using certificates.

To change communication preferences:

- 1 On the **Edit** menu, click **Preferences**.
- 2 Click **ETEMS** to expand the tree, and then click **Communications**.

Communications

Communication timeout (in seconds)

Software upgrade timeout (in seconds)

Use TLS

Use Strict Certificate Authentication

Enable Online Certificate Status Protocol (OCSP)

OCSP Responder Certificate Distinguished Name

Verify OCSP Responder

Ignore Failure To Respond

Revert to CRL on OCSP Responder Failure

Check OCSP Responder Certificate Chain

OCSP URL

Ignore CRL access failure

CRL File Location. Leave blank to use certificate specified URL.

Enable Certificate Policy Extensions

Certificate Policy Extension OIDs
e.g. 2.5.29.32.0, 2.16.840.1.101.3.2.1.3.6, ...

- 3 In the Communications window, modify any of the communication preferences (see [Table 24](#) and [Table 25](#)).
- 4 Do one of the following:
 - Click **Apply** to set the new value.
 - Click **Restore Defaults** to reset the timeout to the factory setting.
- 5 Click **OK**.

Table 24 General communication preferences

Preference	Description
Communication timeout	Sets the amount of time that ETEMS waits for a response from an appliance during a standard communication attempt (refreshing status, comparing configurations, loading configurations). The valid range is 1-180 seconds.
Software upgrade timeout	Sets the amount of time that ETEMS allows for a software upgrade on an appliance to complete. The valid range is 60-1,296,000 seconds (15 days).
Use TLS	By default, ETEMS uses TLS to encrypt communications between the management workstation and the appliance's management port. When TLS is enabled, communication between ETEMS and the appliance is encrypted. If you are managing ETEP appliances, TLS must be enabled. ETEMS cannot communication with the ETEP when TLS is disabled.

Table 25 Strict authentication communication preferences

Preference	Description
Use Strict Certificate Authentication	When enabled, all management communications between EncryptTight components is authenticated using certificates. EncryptTight can use TLS with encryption only, or TLS with encryption and strict authentication for added security. For more information about strict authentication, see "Using Enhanced Security Features" on page 261 .
Enable Online Certificate Status Protocol (OCSP)	When enabled, EncryptTight uses the online certificate status protocol (OCSP) to check the validity of certificates. OCSP is an alternative to using CRLs. For more information about OCSP, see "Validating Certificates Using OCSP" on page 289 .
OCSP Responder Certificate Distinguished Name	Specifies the subject name of the certificate for the OCSP responder.
Verify OCSP Responder	Verifies OCSP responses by authenticating the response message with the installed certificate. To use this option, you must install the certificate from the OCSP responder.
Ignore Failure to Respond	When checked, this option allows ETEMS to accept a certificate even when a response to an OCSP query is not received in a timely manner.
Revert to CRL on OCSP Responder Failure	When checked, if EncryptTight does not receive a reply from the OCSP responder or it cannot be reached, EncryptTight reads the certificate to determine the location of a CRL and uses that instead of OCSP to validate the certificate. In this case, if the CRL cannot be accessed, authentication fails.
Check OCSP Responder Certificate Chain	When checked, this option specifies that ETEMS should check every certificate in the responder's chain of trust.
OCSP URL	Specifies a URL to use for the OCSP responder. This option overrides the URL that may be included in the certificate.

Table 25 Strict authentication communication preferences

Ignore CRL access failure	When enabled, allows EncryptTight to set up communication with a component even when it cannot access the certificate revocation list (CRL) associated with the certificate presented by the component. This option is enabled by default. Note that if OCSP is enabled, this option is invalid and not available. For more information about CRLs, see “Validating Certificates Using CRLs” on page 287 .
CRL File Location	Specifies the location on the management workstation where you want to store CRLs.
Enable Certificate Policy Extensions	Specifies that EncryptTight checks certificates for the presence of the certificate policies extension and enforces the restrictions specified, if any. For more information on certificate policy extensions, see “Configuring the Certificate Policies Extension” on page 269 .
Certificate Policy Extension OIDs	After you enable certificate policies extension, enter the allowed OIDs in the box, separating each with a comma.

7 Provisioning Appliances

This section includes the following topics:

- [Provisioning Basics](#)
- [Appliance User Management](#)
- [Working with Default Configurations](#)
- [Provisioning Large Numbers of Appliances](#)
- [Shutting Down Appliances](#)

Provisioning Basics

EITEMS is the appliance management component of the EncrypTight software. It is a configuration and management tool that lets you provision all of your EncrypTight appliances from a central location.

There are two basic steps to perform when setting up a new appliance. First, add the appliance to EITEMS and define its configuration settings. Then, push the configuration settings to the appliance.

When configuring a new appliance, the first thing to do is select its product family and software version. EITEMS displays a configuration screen tailored to the specified appliance model and software version. On most appliance models the **Interfaces** tab contains the fields required to identify an appliance: its name, password access to the appliance (on applicable models), and the interface IP addresses. On ETEPs with software version 1.6 and later, you can also specify the licensed throughput speed on the Interfaces tab.

Select other tabs to configure additional items on the appliance, such as EncrypTight settings or logging. The availability of specific tabs and configuration options varies depending on your appliance model and software version.

Other than the interface IP addresses, many appliance settings will be the same for all EncrypTight appliances in your network. For these cases EITEMS lets you customize the default configuration to use on your appliances. This offers a significant time savings if you are provisioning a large number of appliances. Another time-saving feature that is useful in large deployments is EITEMS's ability to import configurations from a comma-separated values (CSV) file.

Related topics:

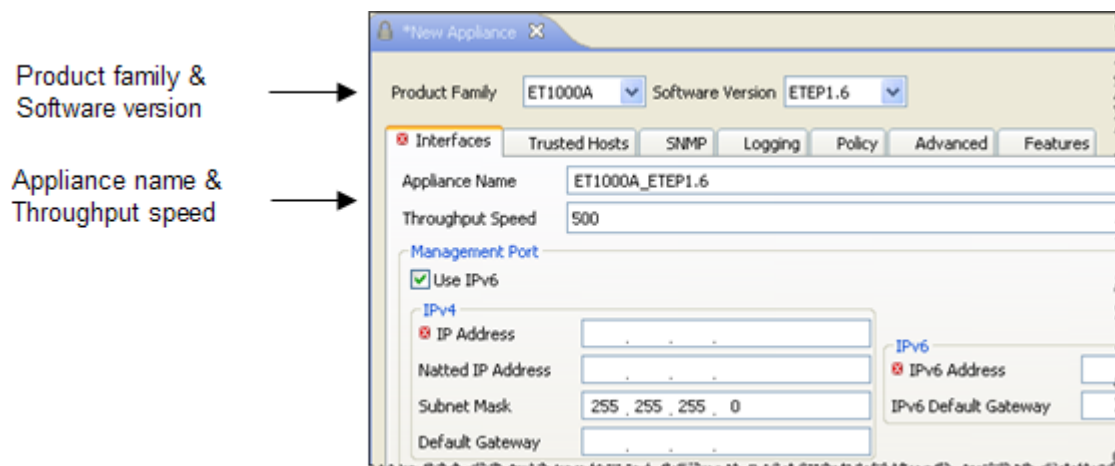
- [“Adding a New Appliance” on page 96](#)

- [“Pushing Configurations to Appliances” on page 97](#)
- [“Working with Default Configurations” on page 110](#)
- [“Provisioning Large Numbers of Appliances” on page 111](#)

Adding a New Appliance

Adding a new appliance in ETEMS is the first step in being able to manage it remotely. Configuration screens are tailored to a particular combination of hardware and software, so it is important to select the correct product family and software version when adding a new appliance.

Figure 26 New Appliance editor for the ET1000A



To add a new appliance:

- 1 On the **File** menu, click **New Appliance**.
- 2 In the appliance editor, select the product family and software version of the new appliance. The appropriate configuration screen appears for your selection.
- 3 Enter the appliance name, which uniquely identifies the appliance in ETEMS.
- 4 For ETEPs with software version 1.6 or later, enter the throughput speed at which you want the ETEP to run. The throughput speed varies according to the ETEP model and the license that you purchased. For more information about licenses, see [“Managing Licenses” on page 56](#).
- 5 Define the appliance configuration and save it. For information about appliance-specific settings see the appliance configuration chapters of this document.
- 6 Push configurations to the appliances.
- 7 Refresh the appliance status.
- 8 Add users and passwords.

Related topics:

- [“Saving an Appliance Configuration” on page 97](#)
- [“Pushing Configurations to Appliances” on page 97](#)
- [“Viewing Appliance Status” on page 98](#)
- [“Appliance User Management” on page 102](#)


- [“Provisioning Large Numbers of Appliances” on page 111](#)
- [“Provisioning PEPs” on page 147](#)

Saving an Appliance Configuration

You can save an appliance configuration at any time during the configuration process. Appliance configurations are saved as part of the EncrypTight workspace. Unsaved changes are indicated with an asterisk on the editor tab.


EEMS provides several ways to save appliance configurations.

Table 26 Saving appliance configurations

Action	Description
Save and New (in the New Appliance editor)	Saves the configuration in the active appliance editor and opens a fresh New Appliance editor. The second appliance editor window retains the settings from the first appliance with the exception of the appliance name and management IP address, which must be unique for each appliance.
Save (in the New Appliance editor)	Saves the configuration in the active appliance editor.
	Saves the configuration in the active appliance editor.
File > Save	Saves the configuration in the active appliance editor.
File > Save all	Saves pending changes in all open appliance editors.

To close open editors without saving the configurations, click **File > Close** or **File > Close All**. Click **no** when prompted to save your changes.

NOTE

EEMS will not save a configuration that contains an error. EEMS indicates the tab and the field that contains the error with .

Related topic:

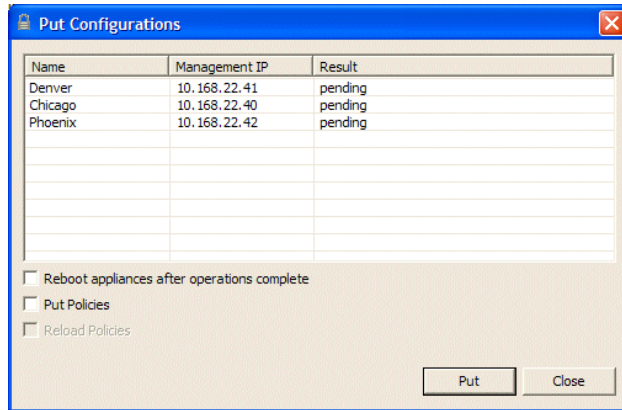
- [“Working with the EncrypTight Workspace” on page 69](#)

Pushing Configurations to Appliances

After defining the configuration for each EncrypTight appliance, you will push the configurations to the targeted appliances in a *put* operation. On some appliance models you can also push a policy file during a put operation.

To push EEMS configurations to appliances:

- 1 In the Appliance Manager, select the target appliances in the Appliances view. Use SHIFT+click to select a contiguous block of appliances; use CTRL+click to select non-contiguous appliances.
- 2 On the **Tools** menu, click **Put Configurations**.



- Optionally, for ETEP appliances with software version 1.6 and later, click **Put Throughput License** to install a license as part of the operation. You can also install a license separately from the Put Configuration operation. To learn more about licenses and throughput speeds, see [“Managing Licenses”](#) on page 56.
- In the Put Configurations window, click **Put** to push configurations, and policies if applicable. The results are shown in the Result column. Common results are shown in [Table 27](#).
- Click **Close** to return to the Appliances view, and then refresh the appliance status (**Tools > Refresh Status**). If you chose to reboot the appliances after loading the configurations, wait a few minutes for the reboot operation to complete before refreshing the status.

Table 27 Put configuration status

Result	Description
Pending	The appliance is selected, but the configuration has not yet been pushed.
OK	The configuration was successfully pushed to the appliance.
Operation failed: [reason]	A problem was encountered during the put operation. ETEMS provides a brief description of the reason for the failure.
Reboot Needed	Some configuration items require a reboot to take effect.

Related topics:



- [“Viewing Appliance Status”](#) on page 98
- [“Comparing Configurations”](#) on page 100

Viewing Appliance Status

The Appliance Manager lists the appliances that ETEMS is managing. It shows information about each appliance, such as its operational status, IP addresses, product family and software version, and date and time. See [Table 29](#) for a description of these fields.

Figure 27 Appliances view

Name	Management...	Speed (MBit)	Last Comm Attempt	Sys Location	Model	Software Revision
Branch1	198.51.100.20	100	03-07-11 03:11	Pittsburgh	ETD100A	ETEP 1.6
Branch2	198.51.100.30	100	03-07-11 03:11	Chicago	ETD100A	ETEP 1.6
Branch3	192.168.1.224	10	03-07-11 10:14	Dallas	ETD010A	ETEP 1.6
Central Office	198.51.100.10	1000	03-07-11 03:10	New York	ET1000A	ETEP 1.6
KAP Main	192.168.224...		never		ETKMS	ETKMS 1.9

By default, automatic status refresh is disabled. You can refresh the status manually by selecting the target appliances and clicking the Refresh Status button . If you prefer, you can have ETEMS automatically poll the status of the appliances. If the appliance status is anything other than , take action as described in [Table 28](#).

To configure automatic status checking:

- 1 On the **Edit** menu, click **Preferences**.
- 2 In the Preferences window, expand the ETEMS listing and select Status.
- 3 Click **Enable automatic status refresh** to have ETEMS automatically refresh the status of the appliances. Clear the check box to disable the feature.
- 4 If you enabled automatic status checking, enter the interval in minutes in the **Refresh Interval** box. The default refresh interval is 60 minutes and can be changed in one minute increments from 1 to 10,080 minutes (7 days).
- 5 Click **Apply**, and then click **OK**.

Table 28 Appliance status indicators








Status Indicator	Description
	Unequal configurations. The ETEMS configuration differs from the configuration stored on an appliance. Compare configurations to view discrepancies (see page 100).
	OK. The ETEMS and appliance configurations are the same, and the appliance is reachable.
	Appliance reboot required (see page 101).
	Reload policies required for policies to take effect (see page 412).
	Status unknown. The appliance is not responding to ETEMS's attempts to communicate with it (see page 224), or ETEMS hasn't yet queried the appliance status.
	Appliance unmanageable due to an incompatible hardware/software combination (see page 226).
	The appliance is in an error state. See the Installation Guide for your appliance model for information about error recovery.

Table 29 The Appliances view summarizes the appliance configurations stored in ETEMS

Field	Description
Name	A unique name that identifies an appliance to ETEMS.
Management IP	The IP address assigned to the appliance's management port. This is the address that ETEMS uses to manage the appliance.
Remote IP	The IP address assigned to the appliance's remote port, which connects the appliance to an untrusted network. This setting is displayed only for appliance models on which the remote IP address is user-configurable.
Last Comm Attempt	Indicates the date and time that ETEMS most recently communicated with the appliance, whether to refresh status, perform a compare operation, push configurations, or upgrade software. This information persists across ETEMS sessions.
Sys Location	The system location is configured on the SNMP tab in the Appliance editor. It is an optional configuration item used to describe the location of the appliance.
Model	The hardware model of the EncryptTight appliance.
Software Revision	The software version of the appliance. With a new appliance configuration, the software version reflects the two-digit version selected in ETEMS. After ETEMS has communicated with the appliance, this field displays the third digit of the software version that is running on the appliance, when available. For example, a new appliance may be added to ETEMS as an ETEP running software version 1.4. After ETEMS communicates with the ETEP it will display the third digit of the software version, such as 1.4.3. ETEMS does not automatically reflect software updates between two digit software versions because of differences in the feature sets (1.4 to 1.5, for example). For feature update releases, you can update the software version in ETEMS using the Multiple Configurations editor.
Date/Time	The appliance's date and time.

Related topics:

- [“Comparing Configurations” on page 100](#)
- [“Filtering Appliances Based on Address” on page 101](#)




Comparing Configurations

When the ETEMS configuration differs from the appliance configuration, the appliance status is **≠**. ETEMS provides a side-by-side comparison so you can see how the two configurations differ and determine which is correct. After determining the correct configuration, you can either copy settings from the appliance to ETEMS or push the ETEMS configuration to the appliance.

Figure 28 Compare the ETEMS and appliance configurations

Property	ETEMS Configuration	Appliance Configuration
Log Facility Priority:Local2	warning	info
Management Interface: Truste...	TrustedHostEntry {□□Applanc...	TrustedHostEntry {□□}
SNTP Client: Enable	true	false
SNTP Client: NTP Service IP Ad...	10.168.1.8	0.0.0.0
Syslog Servers	SyslogServers {□□ApplianceCo...	SyslogServers {□□}
Appliance Group Id	0	0
Appliance IKE VLAN Tag Enabled	false	false
Appliance IKE VLAN Tag Ident...	1	1
Appliance IKE VLAN Tag Priority	0	0
Appliance Policy Ike Authentic...	PresharedKey	PresharedKey
Appliance Policy Preshared Key	01234567	01234567
Appliance Policy Traffic	EthEncrypt	EthEncrypt
Appliance Role	Primary	Primary
Appliance Setting CLI: Session ...	10	10
Appliance Setting FIPS Enabled	false	false
Appliance Setting Non IP Traffi...	Clear	Clear

To compare and update configurations:

- 1 In the Appliance Manager, select an appliance in the Appliances view.
- 2 In the **Tools** menu, click **Compare Config to Appliance** to see a comparison of the ETEMS and appliance configurations. The items that differ are listed first. Click  to toggle between a display of all settings and only those that are different. Some configuration items contain too much information to display on a single line. To view complete information for a truncated item, highlight the item and click **Details** at the bottom of the window.
- 3 Do one of the following:
 - To copy configuration settings from the appliance to ETEMS, select the items to copy and click . The status changes to  to indicate that the configuration items are synchronized.
 - To copy the ETEMS configuration to an appliance, select the appliance and click **Tools > Put Configurations**.
- 4 Click **OK** to save the updated ETEMS configuration.


Related topic:

- [“Pushing Configurations to Appliances” on page 97](#)

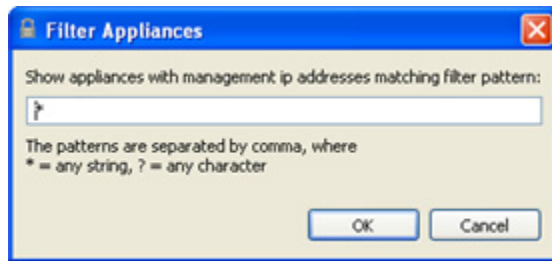
Filtering Appliances Based on Address

To limit the number of appliances that are displayed in the Appliances view, you can filter them based on management IP addresses. This allows you to focus on appliances in a particular network segment.

To apply a filter to the appliances in the Appliances view:

- 1 In the Appliances view, click the filter button in the upper right corner .
- 2 In the Filter Appliances window, enter the filter criteria and then click **OK**. Only the appliances that match the filtering criteria are displayed.

When entering a filter pattern, use an asterisk to filter on any string, and a question mark to filter on any character. You can enter a list of filter expressions, separating each with a comma.



- 3 To restore all appliances in the Appliances view, enter a single asterisk in the Filter Appliances window and then click **OK**.

Rebooting Appliances

Appliances must be rebooted for some configuration changes to take effect, and after installing a software update. Because rebooting interrupts the security policies running on the appliance, carefully consider the best time to reboot the appliances.




CAUTION

Rebooting halts operations on the EncryptTight appliance and interrupts the data traffic on its local and remote ports. Rebooting takes several minutes. During this time all traffic is discarded.

To reboot appliances:

- 1 In the Appliance Manager, select the target appliances in the Appliances view.
- 2 On the **Tools** menu, click **Reboot**.
- 3 Click **OK** to confirm that you want to reboot the selected appliances.

To check the status of an appliance following a reboot, select the appliance and click **Refresh** . The status indicator displays the current state of the appliance.

Appliance User Management

This section discusses user accounts for the ETEP appliances. These accounts are unique to the ETEP and should not be confused with user accounts for the EncryptTight software or external ETKMS.

Related topics:

- [“ETEP User Roles” on page 102](#)
- [“Configuring the Password Enforcement Policy” on page 103](#)
- [“Managing Appliance Users” on page 106](#)
- [“How EncryptTight Users Work with ETEP Users” on page 67](#)

ETEP User Roles

The user role determines how a user can access the appliance and what tasks the user can perform once logged in. Users are assigned a role and a password that allows them to access the functionality of the

appliance that is available to that role. The ETEP can track appliance events based on user name, such as user account activity and policy deployments.

The ETEP has two roles: Administrator and Ops. The Administrator manages the appliance using the EncrypTight software. The Administrator configures the appliance, and creates and deploys policies. The Ops users is only able to log in to the CLI and has access to a limited set of commands.

Table 30 Appliance roles for ETEPs v 1.4 and later

Function	Administrator	Ops
Manage passwords and users	Yes	No
ETEMS access	Yes	No
CLI access	Yes	Yes (subset of commands)

The Administrator assigns user names, passwords and roles for all users. When first installing the ETEP, use the default Administrator password to log in, as shown in [Table 31](#). It is strongly recommended that the Administrator change the default passwords before putting the ETEP into operation in the network.

Table 31 Default user names and passwords on the ETEP

Role	Default user name	Default password
Administrator	admin	admin
Ops	ops	ops

You must maintain at least one Administrator user account on the ETEP in order to manage the appliance. You can add as many user accounts to the ETEP as you need. The ETEP does not impose a cap on the number of user accounts that can be added.

Configuring the Password Enforcement Policy

ETEP 1.6 and later allows you to choose whether to use the default password enforcement policy or strong password enforcement. This option is configured on the Advanced tab. Prior to adding appliance users, configure the password policy on the target appliances. If you plan to configure users and passwords for multiple appliances at once, make sure that the target appliances are enforcing the same password strength policy (strong or default).

The password strength policy determines the following:

- Strength of password rules and conventions
- Password expiration period, expiration warning notification, and grace period
- Maximum number of concurrent user logins allowed

The default password controls are less stringent than the strong password controls, and use standard values for password expiration and maximum number of user logins. The default password controls are enforced on the ETEP unless you explicitly enable strong enforcement.

Earlier version of ETEP software enforce only the default password conventions.

Related topics:

- [“Adding ETEP Users” on page 106](#)
- [“Password Strength Policy” on page 327](#)

User Name Conventions

Follow the guidelines below when creating user names. These conventions apply regardless of the password strength policy.

- User names can range from 1-32 characters.
- Valid characters are alpha and numeric characters (a-z, 0-9), _ (underscore), and - (dash).
- User names must start with an alpha character or an underscore. The first character cannot be a numeric digit or a dash.
- Only lower case alpha characters are accepted.
- User names cannot contain a space.

Default Password Policy Conventions

The following guidelines apply to the default password strength policy.

- Passwords must be a minimum of 8 characters.
- Passwords are case-sensitive.
- Standard alphanumeric characters are allowed. Printable keyboard character and symbols are allowed *except* for the following: < > & “ \$ ‘ () | ; ? / \
- Passwords must contain at least 2 characters from a mix of upper case letters, lower case letters, numbers and non-alphanumeric symbols. For example, an acceptable password might contain an upper case letter and a number, or a lower case letter and a symbol, or an upper case letter and a lower case letter.
- Do not use non-printable ASCII characters.
- Do not use dictionary words. ETEMS does prevent the use of dictionary words, but a password containing a dictionary word will be rejected by the ETEP.

EncryptTight and the ETEP allow an unlimited number of failed login attempts without locking the user out of the appliance.

Strong Password Policy Conventions

Passwords must conform to the following conventions when strong password enforcement is enabled on the ETEP. Strong password controls are available in ETEP 1.6 and later.

- Passwords must be at least 15–256 characters long.
- Standard alphanumeric characters are allowed. Printable keyboard character and symbols are allowed *except* for the following: < > & “ \$ ‘ () | ; ? / \
- Passwords must contain a mix of upper case letters, lower case letters, numbers and special characters, including at least two of each of the four types of characters (2 upper case, 2 lower case, 2 numbers, and 2 special characters).
- When a password is changed, the new password must differ from the previous password by at least four characters.
- The password must not contain, repeat, or reverse the associated user ID.
- The password must not contain three of the same characters used consecutively.
- A user's password must not be identical to any other user's password.
- A new password must be different from the previous 10 passwords used.

- Do not use dictionary words. ETEMS does prevent the use of dictionary words, but a password containing a dictionary word will be rejected by the ETEP.

In addition, the Administrator can place limits on the following:

- Password expiration period, expiration warning notification, and grace period.
- Maximum number of login sessions allowed per user

The ETEP allows three consecutive failed login attempts in a 15 minute period prior to locking an account. After the third failure the account is locked for 15 minutes. The Administrator can unlock a disabled account from the CLI.

Related topics:

- [“Default Password Policy Conventions” on page 104](#)
- [“Adding ETEP Users” on page 106](#)
- [“Password Strength Policy” on page 327](#)

Cautions for Strong Password Enforcement

The password expiration feature puts you at risk for a lockout under certain circumstances. Review the guidelines below to avoid unintended lockouts.



If the Administrators' passwords expire, all Administrator functionality is lost, including the ability to assign a new password. The only means of resetting the password is to reformat the ETEP, which reverts all configurations to their default shipping settings. Reformating the ETEP requires factory service.

Upgrading Software

To avoid having strong passwords expire during an upgrade process, we recommend minimizing the time period between a software upgrade operation and reboot.

If you plan to wait a day or more between an upgrade and reboot, disable strong passwords prior to performing the upgrade. After the upgrade and reboot are complete, re-enable strong passwords.

Note the following:

- Passwords changes that are made between a software upgrade and subsequent reboot do not persist through the reboot. The password expiration timer does not know if a password is changed during that window, placing you at risk of a lockout.
- If all administrator account passwords expire, the unit must be returned to the factory.

Removing ETEPs From Service

To avoid having strong passwords expire during a planned service outage or equipment redeployment, disable strong passwords prior to removing the ETEP from service.

If the password expiration and grace period is exceeded for all administrator accounts while the ETEP is out of service, all users will be locked out and the ETEP must be returned to the factory.

Managing Appliance Users

You can add, modify, and delete appliance users directly from ETEMS. You can update user accounts for a single appliance or for a group of appliances. When managing users, changes take effect immediately. There is no need to push the user data to the ETEP.

Changing appliance user names and passwords can affect EncrypTight's ability to communicate directly with the ETEP. See [“How EncrypTight Users Work with ETEP Users” on page 67](#) to learn more about the interaction between EncrypTight users and ETEP users.

Related topics:

- [“How EncrypTight Users Work with ETEP Users” on page 67](#)
- [“Configuring the Password Enforcement Policy” on page 103](#)
- [“Adding ETEP Users” on page 106](#)
- [“Modifying ETEP User Credentials” on page 108](#)
- [“Deleting ETEP Users” on page 108](#)
- [“Viewing ETEP Users” on page 109](#)

Adding ETEP Users

For security purposes, we recommend replacing the default users and passwords on the ETEP. To ensure your ability to communicate with the ETEP, set up the new users prior to deleting the default account. You can add user accounts for a single appliance or for a group of appliances.

ETEP 1.6 and later includes several enhanced security options:

- Configure password expiration settings. These settings apply when strong password enforcement is enabled on the Advanced tab of the appliance editor. When the default password policy is enforced, the password expiration options are not visible. The default password policy values shown in [Table 32](#) cannot be modified by the Administrator.
- Use a common access card (smart card) to provide user authorization in addition to certificate-based authentication in an EncrypTight deployment. When this feature is enabled, you are required to associate a common name with the ETEP user. See [“Using a Common Access Card” on page 294](#) to learn how to enable this feature across the components of your EncrypTight system.

To add a user to the ETEP:

- 1 In the Appliance Manager, select the target appliances in the Appliances view.
- 2 On the **Tools** menu, click **Appliance User > Add User**.
- 3 In the Add Appliance User window, enter the user name conforming to the conventions listed in [“User Name Conventions” on page 104](#).
- 4 If EncrypTight is configured to use Common Access Card Authentication, enter the common name from the Common Access Card's identity certificate. You will not see this field if the feature is disabled.
- 5 Enter the password for the user, then reenter to confirm it. The password conventions are dependent on the password strength policy that is in effect for the ETEP.
- 6 Select the role to be associated with the user. Admin is the only role that can manage ETEPs from EncrypTight.

- 7 On appliances that are enforcing strong passwords, configure the password expiration settings as described in [Table 32](#).
- 8 Click **Apply** to send the user credentials to the selected appliances. The change takes effect immediately.

Table 32 Password policy values

Parameter	Default password policy	Strong password policy
Password expiration	99999 days	Default is 60. Range is 1-60.
Notify before expiration	7 days	Default is 10. Range is 1-30.
Expiration grace period The number of days after expiration that a user can login with the old password.	0 days	Default is 10. Range is 1-30.
Password change waiting period Minimum number of days a user must wait before changing the password.	0 days	Default is 1. Range is 1-7.
Max simultaneous log-in sessions The maximum number of concurrent sessions allowed for a user.	Unlimited	Default is 2. Range is 1-5.

Figure 29 Adding a user to the ETEP using strong password controls

Add Appliance User

User Credentials

Name:

Password:

Reenter Password:

Role:

Password expiration (days):

Notify before expiration (days):

Expiration grace period (days):

Password change waiting period (days):

Max simultaneous log-in sessions:

Name	Management IP	Result
1c69	192.168.1.69	pending
110c04	10.168.110.4	pending
110c03	10.168.110.3	pending

Related topics:

- [“ETEP User Roles” on page 102](#)
- [“User Name Conventions” on page 104](#)
- [“Default Password Policy Conventions” on page 104](#)
- [“Strong Password Policy Conventions” on page 104](#)
- [“Using a Common Access Card” on page 294](#)
- [“Password Strength Policy” on page 327](#)

Modifying ETEP User Credentials

From the Appliance Manager, you can modify the password or role associated with an ETEP user. You can update user accounts for a single appliance or for a group of appliances. If strong password enforcement is enabled on the ETEPs, you can also modify the password expiration settings.

To modify ETEP user credentials:

- 1 In the Appliance Manager, select the target appliances in the Appliances view.
- 2 On the **Tools** menu, click **Appliance User > Modify User**.
- 3 In the Modify User Credentials window, enter the name of the user that you wish to modify.
- 4 Enter the common name, if applicable.
- 5 Enter the new password for the user, and then reenter it to confirm.
- 6 Change the user’s role, if desired.
- 7 Modify the password expiration settings, if applicable. See [Table 32](#) for a description.
- 8 Click **Apply**. The change takes effect on the appliance immediately.

Related topics:

- [“ETEP User Roles” on page 102](#)
- [“Configuring the Password Enforcement Policy” on page 103](#)
- [“Adding ETEP Users” on page 106](#)

Deleting ETEP Users

You can delete an appliance user on a single appliance or on a group of appliances. The user is removed immediately upon completing the procedure below.

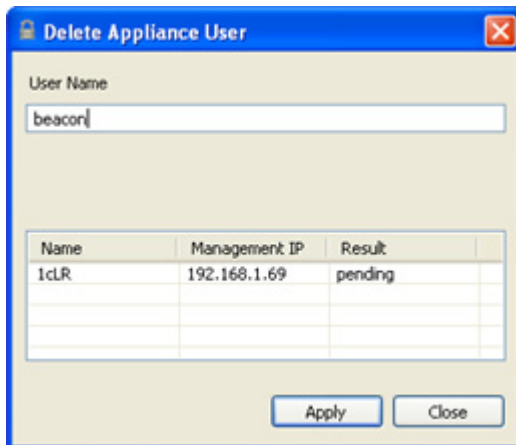
The ETEP prevents you from deleting the default Administrator account (admin/admin) until you have established an alternate Administrator account. It also prevents you from deleting the only remaining Administrator account on the appliance.



We recommend that you store your passwords in a safe place. If you are unable to log in to the ETEP with a valid Administrator user name and password, the ETEP must be returned to the factory to be reset.

To delete a user from the ETEP:

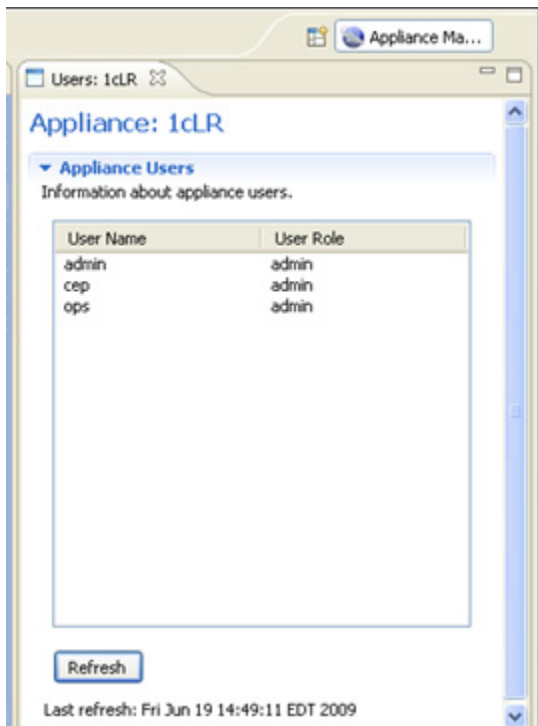
- 1 In the Appliance Manager, select the target appliances in the Appliances view.
- 2 On the **Tools** menu, click **Appliance User > Delete User**.
- 3 In the Delete Appliance User window, enter the user name that you wish to delete.
- 4 Click **Apply**. The user is immediately removed from the target ETEPs.

Figure 30 Delete an appliance user**Viewing ETEP Users**

You can check the user accounts that are configured on a particular ETEP by selecting **View > Appliance Users**. The Users view lists the user name and role for each user on the appliance. Passwords are not displayed. To update the User view data, click **Refresh**.

Password expiration settings can be viewed from the CLI (user-config level **show** command).

Figure 31 The Users view displays the user accounts configured on the ETEP



Working with Default Configurations

Each appliance requires a unique name and management port IP address, but many other settings will be the same across all appliances. ETEMS lets you define your own set of default settings to be used in all appliances of particular model and software version level. See the configuration chapter for your appliance model for more information about each configuration option.

Related topics:

- [“Customizing the Default Configuration” on page 110](#)
- [“Restoring the ETEMS Default Configurations” on page 111](#)

Customizing the Default Configuration


You can think of a default configuration as a template that contains settings to be used on all appliances. Using a customized default configuration offers a significant time savings when you are provisioning a large number of appliances. Add settings that are common to all appliances of a particular model and software version, such as the NTP server, EncryptTight settings, syslog servers, or the password that ETEMS uses to access the appliances.

To customize the default configuration:

- 1 On the **Edit** menu, click **Default Configuration**.
- 2 Select the product family and software version.
- 3 In the appliance editor, change the desired defaults on each tab.

- 4 Click **OK**.

**NOTE**

ETEMS will not save a default configuration that contains an error or an invalid entry. The OK button is disabled if an error is detected. ETEMS indicates the tab and the field that contains the error with .

Restoring the ETEMS Default Configurations

For each product family/software version combination, you can replace a custom default configuration with the ETEMS factory default configuration. The following items are unaffected by restoring the factory default configuration:

- Password
- Appliance name
- Management IP address
- Remote port IP address (on applicable appliances)
- Certificates
- Policies created using EncrypTight ETPM

To return the default values to factory settings:

- 1 On the **Edit** menu, click **Default Configurations**.
- 2 Select an appliance model and software version level from the list.
- 3 In the appliance editor, click **Use Factory**.
- 4 Click **OK** to save the factory settings as the defaults and return to the Appliances view.

Consider the following items before pushing a factory default configuration to an appliance:

- Settings that affect traffic are changed when the factory settings are restored. On some appliance models these changes require a reboot, which interrupts traffic on the data ports.

**CAUTION**

Restoring the default configuration may change traffic-affecting settings or require rebooting the appliance.

Provisioning Large Numbers of Appliances

If you have a lot of appliances to add to ETEMS, entering each configuration individually through the appliance editor can be time-consuming. ETEMS offers some tools for streamlining appliance provisioning in large deployments. The workflow is as follows:

- 1 Create a customized default configuration, which will serve as a template, for each appliance model / software version combination that you need.
- 2 Add the new appliances in ETEMS by entering the basic appliance information in a CSV file and then importing the data into ETEMS.
- 3 Push the configurations to the appliances.
- 4 Check the appliance date and time.

Related topics:

- [“Creating a Configuration Template” on page 112](#)
- [“Importing Configurations from a CSV File” on page 112](#)
- [“Changing Configuration Import Preferences” on page 115](#)
- [“Checking the Time on New Appliances” on page 116](#)

Creating a Configuration Template

A default configuration is like a template that contains common settings to be used on all appliances of a particular hardware model and software version. Using a customized default configuration can save a lot of time when you are provisioning a large number of appliances.

If you have two types of appliances in your network—for example, ET0100As running ETEP1.6 software and ET0010As running ETEP1.5 software—you can create two templates, one for the 1.6 ETEPs and another for the 1.5 ETEPs. In each template, add the settings that are common to each appliance type, such as local and remote port auto-negotiation and link speed settings, log settings and syslog servers, NTP server, EncryptTight settings, and the password that ETEMS uses to communicate with the appliances. After the default configurations are created and saved, any new appliances of that hardware/software type will have the defaults settings included, eliminating the need to re-enter that data.

Related topic:

- [“Working with Default Configurations” on page 110](#)

Importing Configurations from a CSV File

When you have a large number of appliances to add to ETEMS, you can save time by entering the basic appliance information in a CSV file and then importing the data into ETEMS. Take note of the following guidelines and restrictions for importing configurations:

- Passwords
Use the default password **admin** when importing configurations, and then use ETEMS to configure user names and passwords after the import.
- Local and remote port addresses
On ETEPs, remote and local interface addresses are optional configuration items. They are needed when operating the ETEP in non-transparent mode to use the virtual IP feature in EncryptTight. If you are operating in transparent mode, you do not need to enter these addresses.
See [“Importing Remote and Local Interface Addresses” on page 114](#) for more information about remote and local interface formatting.

 **NOTE**

If you are importing configurations for ETEPs with software version 1.6 or later, or you intend to upgrade the ETEPs that you are importing to software version 1.6 or later, make sure your EncryptTight license covers the additional ETEPs. After the import, you need to set the appropriate throughput speeds on the ETEPs and install licenses. If you attempt to set throughput speeds that are faster than the license allows, ETEMS will mark the configuration as being in error and you will not be able to save it.

To create the import file, enter the data in Excel and save it as .csv file or enter the data directly in Notepad. You must adhere to the formats shown in [Figure 32](#) and [Figure 33](#). The first line in the file

specifies the document type, which ETEMS needs to successfully import the file. The pound symbol (#) indicates a comment line, and is ignored by ETEMS during the import operation. In the CSV file, commas are used to delineate one field from the another.

Figure 32 Import document format in Excel

	A	B	C	D	E	F
1	DocumentType=simple					
2	#deviceType	softwareVersion	name	ipAddress	subnetMask	ipDefaultGateway
3	et0100a	etep1.6.0	Toronto_CA	192.168.224.11	255.255.255.0	192.168.224.10
4	et0100a	etep1.6.0	Madrid_ES	192.168.224.21	255.255.255.0	192.168.224.20
5	et0100a	etep1.6.0	Taipei_TW	192.168.224.31	255.255.255.0	192.168.224.30
6	et0100a	etep1.6.0	Chicago_US	192.168.224.41	255.255.255.0	192.168.224.40
7						

Figure 33 Import document CSV file in Notepad

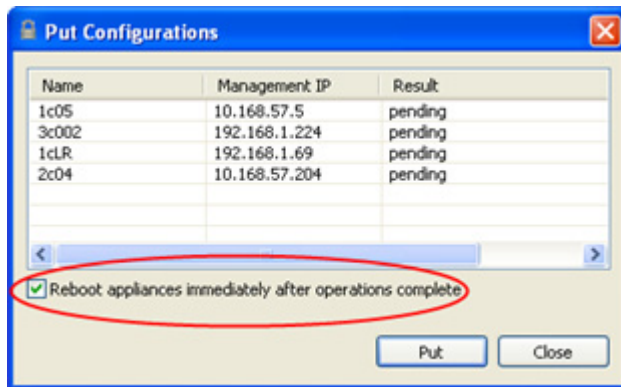
```
DocumentType=simple
#deviceType,softwareVersion,name,ipAddress,subnetMask,ipDefaultGateway
et0100a,etep1.6.0,Toronto_CA,192.168.224.11,255.255.255.0,192.168.224.10
et0100a,etep1.6.0,Madrid_ES,192.168.224.21,255.255.255.0,192.168.224.20
et0100a,etep1.6.0,Taipei_TW,192.168.224.31,255.255.255.0,192.168.224.30
et0100a,etep1.6.0,Chicago_US,192.168.224.41,255.255.255.0,192.168.224.40
```

Table 33 Import document format description

Attribute	Description
DocumentType=	ETEMS requires the document type to be defined as “simple” when importing a CSV configuration file.
deviceType	Product Family (appliance model), such as ET0100A or ET0010A. The device type is not case-sensitive.
softwareVersion	Enter the software version as a three-digit number, with the third digit being zero (for example, etep1.5.0). Even if the software installed on the appliance has a non-zero third digit, the third digit must be entered as zero for a successful import. For example, if the software on the ET0100A is v1.5.2, enter the software version as 1.5.0. After the appliance is provisioned and ETEMS communicates with it, ETEMS will accurately display the third digit.
name	Name that uniquely identifies the appliance in ETEMS. The device name is case-sensitive. Spaces are allowed within the name.
ipAddress	Management port IP address, in dotted decimal notation. The address imported into ETEMS should match the management IP address configured on the appliance.
subnetMask	Management port subnet mask, in dotted decimal notation.
ipDefaultGateway	Management port default gateway, in dotted decimal notation. See the Installation Guide for your appliance for more information about setting the IP address, mask, and gateway.

To import appliance configurations to ETEMS:

- 1 Create a CSV file containing the new appliance configuration data.
- 2 In ETEMS, import the configurations (**File > Import Configurations**). If ETEMS detects an error in the CSV file, none of the configurations are imported. ETEMS displays an error message that includes the line in the file that contains the error and a description of the problem.
- 3 Push the configurations to the target appliances and reboot them. In the **Tools** menu, click **Put Configurations**. In the Put Configurations window, select the checkbox labeled **Reboot appliances immediately after operation complete** (Figure 34).

Figure 34 Put configurations and reboot appliances**Related topics:**

- [“Importing Remote and Local Interface Addresses”](#) on page 114
- [“Changing Configuration Import Preferences”](#) on page 115
- [“Transparent Mode”](#) on page 306

Importing Remote and Local Interface Addresses

For ETEPs, remote and local interface addresses are optional configuration items. They are needed when operating the ETEP in non-transparent mode.

The standard CSV import format is as follows:

```
<deviceType>,<softwareVersion>,<appliance name>,<management ip address>,<management subnet mask>,<management default gateway>
```

To include remote and local interface data, append the following information to the same line:

```
,RemoteInterface,<remote ip address>,<remote subnet>[,<remote default gateway>],end,LocalInterface,<local ip address>,<local subnet mask>[,<local default gateway>],end
```

RemoteInterface, **LocalInterface** and **end** are keywords. Keywords are case-sensitive and must be entered exactly as shown in [Table 34](#). If the RemoteInterface keyword is included in the import file, then you must specify the remote port IP address and subnet mask. If you are not defining a remote default gateway address, enter 0.0.0.0. The **end** keyword delineates the end of the attribute list started by the RemoteInterface keyword. Next, enter the LocalInterface keyword followed by the local port IP address and subnet mask. If you are not defining a local default gateway address, enter 0.0.0.0. Complete the statement with the **end** keyword. Sample import statements are shown in [Figure 35](#).

Table 34 Remote and local keywords and attributes

RemoteInterface	Keyword that indicates the beginning of the remote interface definition
remote ip address	Remote port IP address in dotted decimal notation
remote subnet	Remote port subnet address in dotted decimal notation
remote default gateway	Remote port default gateway. If you do not use a default gateway, enter 0.0.0.0.
LocalInterface	Keyword that indicates the start of the local interface definition

Table 34 Remote and local keywords and attributes

local ip address	Local port IP address in dotted decimal notation
local subnet	Local port subnet address in dotted decimal notation
local default gateway	Local port default gateway. If you do not use a default gateway, enter 0.0.0.0.
end	Keyword that indicates the end of the remote interface and local interface definitions

Figure 35 CSV import examples with remote and local interface attributes

```

DocumentType=simple
#etep 1.6 without remote and local interfaces specified
et0100a,etep1.6.0,datacenter,198.39.240.120,255.255.255.0,198.39.240.113

DocumentType=simple
#etep 1.6 with remote and local attributes specified
et0100a,etep1.6.0,datacenter,198.39.240.120,255.255.255.0,198.39.240.113,Re
moteInteface,1.1.1.12,255.255.255.0,1.1.1.1,end,LocalInterface,1.1.1.15,255
.255.240.0,1.1.1.10,end

DocumentType=simple
#etep 1.6 with the optional local port default gateway unspecified
et0100a,etep1.6.0,datacenter,198.39.240.120,255.255.255.0,198.39.240.113,Re
moteInteface,1.1.1.12,255.255.255.0,1.1.1.1,end,LocalInterface,1.1.1.15,255
.255.240.0,0.0.0.0,end

```

When importing a configuration to a new ETEP appliance, specifying the remote and local interface automatically disables Transparent mode. If you are importing a configuration to an existing appliance on which Transparent mode is enabled, you will need to merge the configurations in order for the new import data to be accepted on the ETEP. See [“Changing Configuration Import Preferences” on page 115](#) to learn more about merging new configurations with existing ones.

Related Topics:

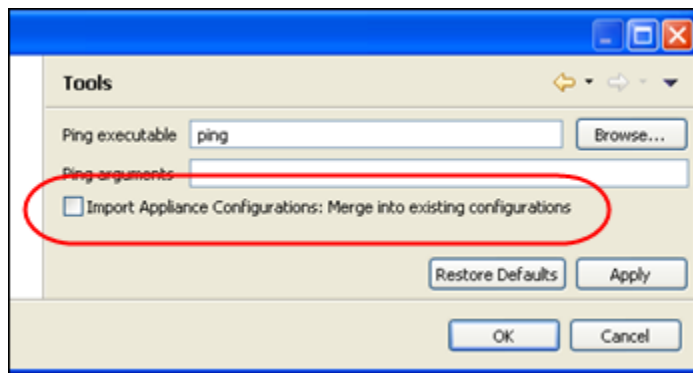
- [“Importing Configurations from a CSV File” on page 112](#)
- [“Changing Configuration Import Preferences” on page 115](#)
- [“Transparent Mode” on page 306](#)

Changing Configuration Import Preferences

In addition to facilitating the provisioning of new appliances, the Import Configurations feature can be used to merge newer configurations with existing ones. First, ETEMS verifies that the appliance name and IP address in the CSV file matches that of an existing configuration. If they match, ETEMS merges the new information with the existing configuration, replacing the updated fields.

This behavior is controlled in the Tools Preferences. The default behavior is to reject duplicate configurations. To enable configuration merging, go to **Edit > Preferences > ETEMS > Tools** and click the checkbox labeled **Import Appliance Configuration: Merge existing configurations**.

The following settings cannot be merged into an existing configuration: appliance name, management IP address, product family (device type), or software version.

Figure 36 Set the preference for importing configurations

Checking the Time on New Appliances

After importing configurations to ETEMS and pushing them to the appliances, refresh the appliance status. In the Appliances View check the date and time of the new appliances. If any of the new appliances' timestamps differ from the management station's time by more than five minutes, edit the appliance to correct the date and time (**Edit > Date**). When the appliance time differs from actual time by more than several minutes, the appliance can have trouble synchronizing with the NTP time server. Time synchronization is essential for proper operation in an EncrypTight deployment.

Shutting Down Appliances

It is important that a proper system shutdown is performed prior to powering off ETEPs. The shutdown operation halts all running tasks on the ETEP and prepares it for being powered off. Failure to perform a shutdown may lead to file system corruption and potential appliance failure. The shut down option is available only on ETEP appliances.

The ETEP remains in a shutdown state until the power is cycled. The shutdown state is indicated with an operational code on the status or diagnostic display as shown in [Table 35](#).

Table 35 Shutdown operational codes

Appliance model	Operational code
ET0010A	2, 3, 4
ET0100A, ET1000A	--

To shut down the ETEP:

- 1 In the Appliance Manager, select the target appliances in the Appliances view.
- 2 On the **Tools** menu, click **Shutdown**.
- 3 Click **OK** to confirm that you want to shut down the selected appliances.

8 Managing Appliances

This section includes the following topics:

- [Editing Configurations](#)
- [Deleting Appliances](#)
- [Connecting Directly to an Appliance](#)
- [Upgrading Appliance Software](#)
- [Restoring the Backup File System](#)

Editing Configurations

When modifying configurations, the following settings have their own unique editors: management IP address, date and time, and password. These items are handled uniquely to avoid conflicts between the appliance configuration and ETEMS that could affect ETEMS's ability to communicate with the appliance. Of these settings, the password and the date and time can be changed for multiple appliance configurations in a single operation. The management IP address is unique to each appliance and therefore is changed for only one appliance at a time.

When editing other configuration settings, use the appliance editor to change values on a single appliance. Several of the most common settings can be changed on multiple appliances in a single operations, using ETEMS's multiple configuration editor.

Related topics:

- [“Changing the Management IP Address” on page 118](#)
- [“Changing the Date and Time” on page 120](#)
- [“Changing the Date and Time” on page 120](#)
- [“Changing Settings on a Single Appliance” on page 121](#)
- [“Changing Settings on Multiple Appliances” on page 121](#)

Changing the Management IP Address

EITEMS uses the appliance's 10/100 Ethernet management port to communicate with the appliance. The management IP address in EITEMS must match the address of the appliance for successful communication. To keep the two configurations in sync you can make either of the following changes:

- Push a new IP address to the appliance from EITEMS (see [“Changing the Address on the Appliance” on page 118](#))
- Update EITEMS with the appliance's new IP address. You need to do this when the management IP address has been changed directly on the appliance (see [“Changing the Address in EITEMS” on page 119](#)).

Changing the Address on the Appliance

You can change the management IP address that is configured on an appliance from EITEMS.

If the appliance supports IPv6 addressing, the editor allows you to change either the IPv4 or IPv6 address, depending on the address preference. If the management port address preference is set to **Use IPv6**, focus is applied to the IPv6 address. Otherwise, focus is applied to the IPv4 address. IPv6 addressing is supported on ETEP appliances that are running software version 1.6 and later.

To change the management IP address on the appliance:

- 1 In the Appliance Manager, select an appliance from the Appliances view.
- 2 On the **Edit** menu, click **Management Address**. The Change Management IP window opens ([Figure 37](#)).
- 3 In the **IP Address To** field, type the management port IP address.
- 4 In the **Subnet Mask To** field, confirm the subnet mask and change if necessary.
- 5 In the **Default Gateway To** field, confirm the default gateway and change if necessary.
- 6 Click **Finish** to apply the new address to the appliance.

When the change is complete EITEMS refreshes the Appliances view. If EITEMS is unable to update the management IP address, it displays the reason for the failure.

Figure 37 Change Management IP window

The screenshot shows two overlapping windows from the 'Change Management IP' dialog. The top window is for IPv4 configuration, and the bottom window is for IPv6 configuration. Both windows have a title bar and a close button. The top window has a red error icon and text: 'IPv6 Address To: IP address cannot be void'. The bottom window has a red error icon and text: 'IPv6 Address To: IP address cannot be void'.

Change Management IP

Enter the new management IP settings for the appliance

IPv6 Address To: IP address cannot be void

IP Address

From: 192 . 168 . 1 . 69

To: 192 . 168 . 1 . 69

Subnet Mask

From: 255 . 255 . 192 . 0

To: 255 . 255 . 192 . 0

Default Gateway

From: 192 . 168 . 1 . 1

To: 192 . 168 . 1 . 1

IPv6 Address

From: 2001:db8::211:11ff:fe58:743/64

To: IP address cannot be void

Default IPv6 Gateway

From: 2001:db8::20f:f7ff:fe84:bfc2

To: 2001:db8::20f:f7ff:fe84:bfc2

Related topics:

- “Changing the Address in ETEMS” on page 119
- “Management Port Addressing” on page 302
- “IPv6 Addressing” on page 304

Changing the Address in ETEMS

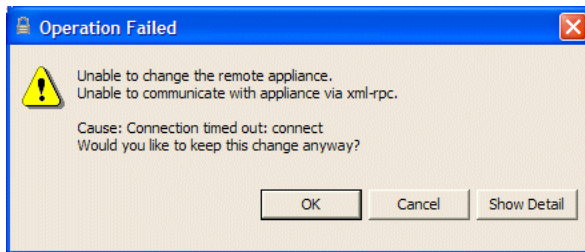
If the management IP address has been changed directly on the appliance, you need to update the address in the ETEMS configuration.

For ETEP 1.6 and later appliances, you can edit the management port IP address directly in the appliance editor. For other appliance models, use the following procedure.

To update ETEMS with the appliance’s new management IP address:

- 1 In the Appliance Manager, select an appliance from the Appliances view.
- 2 On the **Edit** menu, click **Management Address**. The Change Management IP window opens.
- 3 In the **IP Address To** field, type the management port IP address.
- 4 In the **Subnet Mask To** field, confirm the subnet mask and change if necessary.
- 5 In the **Default Gateway To** field, confirm the default gateway and change if necessary.
- 6 Click **Finish**. After a few seconds ETEMS displays an “Operation Failed” message (Figure 38).
- 7 Click **OK** to update ETEMS with the appliance’s new management IP address.

Figure 38 Operation failed message in response to management IP change

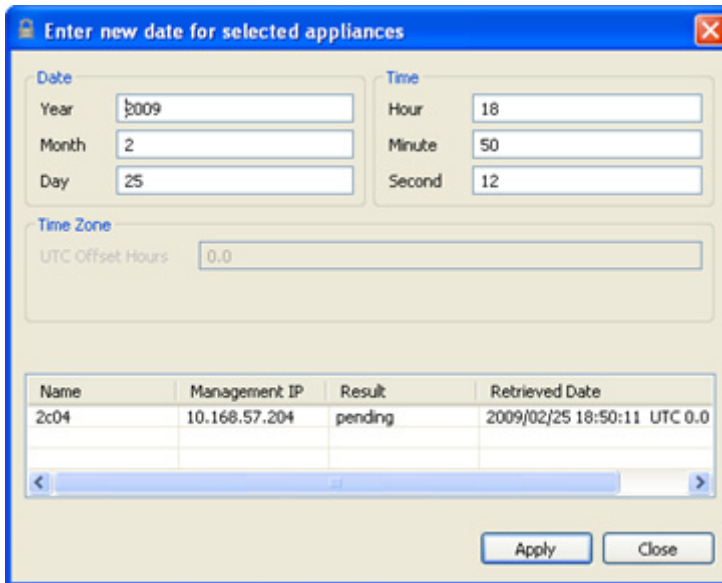


Changing the Date and Time

EITEMS can change the date and time on a single appliance or a group of appliances. On appliance models where the time zone cannot be configured (EETEP or a mix of appliance models), enter the date and time relative to UTC. To calculate the local time relative to UTC, add or subtract the offset hours from UTC for the local time zone (UTC ± n) plus an offset for daylight saving time, if in effect. The following examples give the local time at various locations at 12:00 UTC when daylight saving time is not in effect:

- New York City, United States: UTC-5; 07:00
- New Delhi, India: UTC+5:30; 17:30

Figure 39 New Date window



The default date and time shown in the editable fields of the New Date window are those of the EITEMS management workstation. When editing the date on the EETEP, which has a UTC offset of 0, EITEMS displays the management station time relative to UTC. For example, if the local time is 10:00 am US EST, EITEMS displays the UTC time of 15:00.

 **NOTE**

The SNTP client must be disabled on an appliance in order to change its date or time manually. If SNTP is enabled, the date and time change operation will fail.

To change the date and time:

- 1 Make sure that the SNTP client is disabled on the target appliances. There are two ways to disable the SNTP client setting: from the Appliance editor's Advanced tab, or from the Edit menu, **Multiple Configurations > SNTP Client**.
- 2 In the Appliance Manager, select the target appliances in the Appliances view.
- 3 On the **Edit** menu, click **Date**.
- 4 In the New Date window, enter the new date and time,.
- 5 Click **Apply** to immediately apply the new date and time to the target appliances. The result is displayed for each appliance. If ETEMS is unable to update the appliance's clock, it displays the reason for the failure.

Changing Settings on a Single Appliance

When editing the configuration of a single appliance, use the appliance editor to make changes to all settings other than management IP address, password, and date and time.

To edit the configuration of a single appliance:

- 1 In the Appliance Manager, select an appliance in the Appliances view.
- 2 On the **Edit** menu, click **Configuration**.
- 3 In the appliance editor, modify the configuration settings. To change all of the values to their defaults, click **Use Defaults**.
- 4 When you are done, do one of the following:
 - Click **OK** to save your changes and close the appliance editor.
 - Click **Save** to save your changes and keep the appliance editor open.
- 5 Push the new configuration to the appliance (**Tools > Put Configuration**).

Related Topics:

- [“Pushing Configurations to Appliances” on page 97](#)
- [“Changing Settings on Multiple Appliances” on page 121](#)

Changing Settings on Multiple Appliances

ETEMS allows you to change some settings on multiple appliances in a single operation rather than editing each appliance individually. Settings that are supported by the multiple appliance editor are:

- Data port settings: auto-negotiation, flow control, and link speed
- Policy Settings (Layer 2 or Layer 3, enable/disable EncrypTight)
- Reassembly mode (ETEPs only)
- SNMP community, trap host and trap mask

- SNTP client
- Software version
- Syslog servers

Other settings that can be edited on multiple appliances are date and time, and password. These settings do not use the multiple configurations editor: they have their own unique editors, which are accessed from the Edit menu.

The multiple configuration editor changes the appliance's configuration in the EncrypTight workspace. After editing the appliance configurations, push the configurations to the targeted appliances for the new settings to take effect.

When editing a setting for a group of appliances, ETEMS's multiple configuration editor displays the existing data for the first selected appliance. You can accept those values and apply them to all of the target appliances, or use them as a starting point to make as many changes as you like.

ETEMS allows selecting a mixture of hardware models and software versions *except* when updating the software version, when all selected appliances must be of the same hardware model.

Some options displayed in the editor may be invalid on some of the selected appliances and valid on others. When ETEMS encounters an invalid setting for an appliance or when the new value is the same as the existing value, ETEMS ignores the new value and keeps the existing value for that appliance.

When you finish editing a group of appliances, ETEMS displays a summary of the results, indicating the number of appliance configurations that it changed in the workspace.

To update an appliance setting on multiple appliances:

- 1 In the Appliance Manager, select the target appliances in the Appliances view.
- 2 Click **Edit > Multiple Configurations**. Select an appliance setting from the list.
- 3 In the editing window, update the settings and then click **Apply**.
- 4 From the Appliances view, select the target appliances and push the new configuration to the appliances (**Tools > Put Configuration**).

Related topics:

- [“Changing the Date and Time” on page 120](#)
- [“Changing the Date and Time” on page 120](#)
- [“Changing Settings on a Single Appliance” on page 121](#)

Deleting Appliances

When an appliance is deleted using ETEMS it is removed from the EncrypTight workspace, meaning it cannot be configured and managed using ETEMS. An appliance will continue to execute security policies as long as its properly connected and configured in the network, even after it has been deleted from ETEMS. In most cases, you will delete an appliance from ETEMS when an appliance is removed from service in the field.

To delete appliances:

- 1 In the Appliance Manager, select the appliances to delete in the Appliances view.
- 2 On the **Edit** menu, click **Delete**. A confirmation message displays.
- 3 Click **OK** to confirm the selection and delete the selected appliances.

Connecting Directly to an Appliance

EEMS supports appliance-level tasks on appliances managed by EEMS. You can connect directly to an appliance's command line interface (CLI) to perform troubleshooting and diagnostic tasks and administrative functions.

Related topics:

- [“Connecting to the Command Line Interface” on page 123](#)
- [“Upgrading Appliance Software” on page 123](#)

Connecting to the Command Line Interface

From EEMS you can connect directly to an appliance to issue CLI commands. Two types of commands are available on most appliance models: **show** commands for diagnostics and troubleshooting, and Administrator commands for appliance and user management. See the user manuals for your appliance model for a list of commands and usage guidelines.

To connect to the appliance CLI:

- 1 Make sure that you can connect using the client available for your appliance model. ETEP appliances use SSH to securely connect to the CLI. An SSH client is included with the EncrypTight installer.
- 2 In the Appliance Manager, click the target appliance in the Appliances view to select it.
- 3 On the **Tools** menu, click **SSH** to connect to the appliance's CLI.
- 4 Enter the user name and password to log in to the CLI as **ops** or **admin**. Once you are logged in, you can issue all CLI commands available to your user type.
- 5 When you are finished, type **exit** to log out of the CLI.

Upgrading Appliance Software

Using EEMS, you can download new software from an FTP server to one or many PEPs of the same product family. For example, EEMS can upgrade a mix of ETEP models, such as ET0010As, ET0100As, and ET1000As, in a single operation.

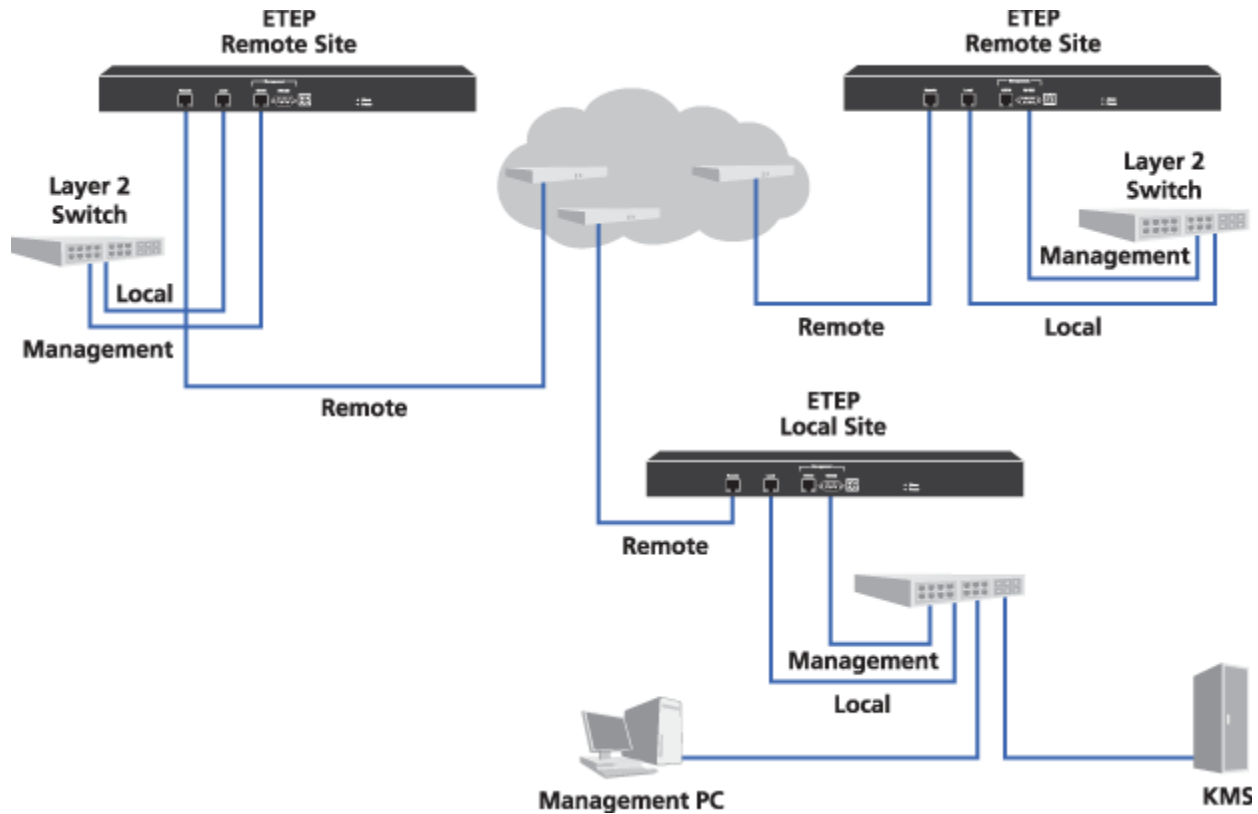
When upgrading software on ETEP 1.6 and later appliances, you have the option of using FTP or SFTP for secure file transfer. If you choose SFTP as the connection method, all of the selected appliances must support SFTP.

Software upgrades on multiple appliances are performed in parallel. EEMS can upgrade groups of 10 appliances at a time. If you select a larger number of appliances to upgrade, as each upgrade completes, EEMS starts upgrading one of the remaining appliances. This continues until upgrades have been initiated on all of the selected appliances.

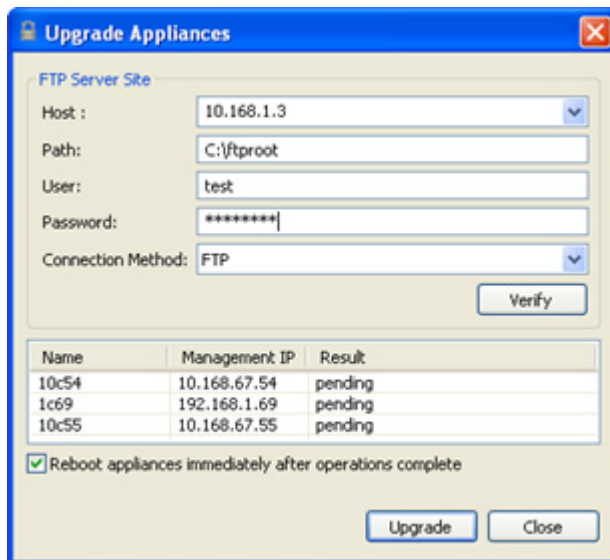
The amount of time it takes to complete a software upgrade depends on the appliance model and speed of the link. The upgrade time increases proportionately to the decrease in the link speed. If software is not successfully loaded to any particular appliance in a predefined time frame, the connection times out. The software upgrade timeout is user-configurable (**Edit > Preferences > ETEMS > Communications**).

Prior to upgrading an appliance, we recommend making a backup copy of the existing file system. If you experience a problem with an upgrade, you can then restore the appliance's file system from the backup copy. A backup is created automatically on ETEP appliances.

Figure 40 Upgrade remote appliances first when managing appliances in-line, where management traffic flows through the data path



If you are managing your EncrypTight appliances in-line as shown in [Figure 40](#), we recommend performing a software upgrade in two stages. First, upgrade all the appliances at remote sites and reboot them. When the remote site appliances are up and operational, upgrade the local site appliance, which is co-located with the ETEMS management station. Upgrading the local appliance at the same time as the remote appliances can cause connectivity with the management station to be lost and the remote site upgrades to fail.

Figure 41 Upgrade software on multiple appliances from a central location**CAUTION**

Appliances must be rebooted for the new software to take effect. Rebooting an appliance interrupts traffic on the data ports for several minutes. During the reboot operation all packets are discarded.

**CAUTION**

For ETEPs, we recommend rebooting immediately after upgrading. Any configuration changes that are made between the upgrade and subsequent reboot will be lost when the appliance reboots. This includes changes to policies and keys (including rekeys), certificates, and appliance configuration.

To upgrade software:

- 1 From the CD for the PEPs that you want to upgrade, copy the folder for your appliance model to your default FTP directory.
For example, if you are upgrading ETEP PEPs copy the ETEP folder to your FTP directory.
- 2 In the Appliance Manager, select the target appliances in the Appliances view. If you are managing the PEPs in-line, upgrade the remote site appliances first before upgrading the data center appliance, as shown in [Figure 40](#).
- 3 On the **Tools** menu, click **Upgrade Software**.
- 4 Enter the **FTP server site** information for the upgrade software, as described in [Table 36](#). Do not use the following special characters in the FTP user name and password: @ : ? # < > &.
Optional. Click **Verify** to confirm that the site is reachable. If it is not, ETEMS displays a message indicating the nature of the problem.
- 5 Decide when to reboot the upgraded appliances. Appliances must be rebooted for the new software to take effect. Select the **Reboot after upgrade** check box to automatically reboot the appliances immediately following a successful upgrade. Clear the check box to reboot the appliances at a later time, for example after working hours. See [“Rebooting Appliances” on page 102](#) for more information about rebooting appliances.

- Click **Upgrade**. ETEMS confirms that the FTP site is reachable before it begins the upgrade operation. Upgrade results for each appliance are displayed in the Result column of the Upgrade Appliances table.

Name	Management IP	Result
San Diego	222.1.1.6	OK
Dallas	222.1.1.2	pending
Phoenix	222.1.1.5	pending

- Upgrading the software version on the appliance does not automatically update the ETEMS configuration. After the appliances have been rebooted, you can edit the ETEMS configurations to reflect the new software version running on the appliances (**Edit > Multiple Configurations > Software Version**).

The appliance will operate properly with the upgraded software regardless of whether the ETEMS configuration is updated to reflect the new software version. However, new configuration options will not be reflected in the Appliance editor until the ETEMS configuration is updated with the new software version.

Table 36 FTP server site information for appliance software upgrades

Field	Description
Host	IP address of the management workstation running the FTP server software. If you are retrieving log files from a host that has already been configured, you can select its IP address from the Host box. ETEMS completes the remaining FTP server information for you based on the selected host IP address. ETEP 1.6 and later appliances support IPv4 and IPv6 addresses. If you are using an IPv6 host address, all of the selected appliances must support IPv6.
Path	The directory on the FTP server that contains the files of interest. Valid entries are the default FTP directory and its subdirectories. Enter the directory listing relative to the default directory. If the files are located in the default directory, leave this field blank.
User	User ID of a user on the FTP server. Do not use the following characters: @ : ? # < > &
Password	Password associated with the user name. Do not use the following characters: @ : ? # < > &
Connection Method	FTP is the default file transfer protocol and is supported on all appliance models and software revisions. SFTP provides secure file transfer. It is supported on ETEP appliances running version 1.6 and later software.

Related topics:

- [“Canceling an Upgrade” on page 127](#)
- [“What to do if an Upgrade is Interrupted” on page 127](#)
- [“Checking Upgrade Status” on page 127](#)
- [“Modifying Communication Preferences” on page 92](#)
- [“Changing Settings on Multiple Appliances” on page 121](#)

Canceling an Upgrade

To cancel a software upgrade that is underway for a series of appliances, click **Cancel**. Appliance upgrades that are in progress will complete their upgrades but no additional upgrades will be initiated. The upgraded appliances will reboot if you selected **Reboot appliances after operations complete**.

For ETEP appliances, the result for the upgrades in progress is listed as “in operation.” Upgrades on appliances that have not yet received the upgrade command are cancelled. Their status is reported as “canceled.”

What to do if an Upgrade is Interrupted

If the upgrade operation is interrupted or times out prior to completion, refer to the results table to see which appliances were successfully upgraded and which were not. For appliances that were not successfully upgraded do the following:

- 1 Make a note of the appliance name and problem description in the **Result** column.
- 2 Close the **Upgrade Appliances** window.
- 3 Fix the problem with the appliance.
- 4 Select the target appliances and restart the software upgrade operation.

Checking Upgrade Status

You can check on the status of an upgrade using two methods:

- In ETEMS, configure a syslog server to receive events generated by the ETEP. Several system log events with a priority level of “notice” are generated by the ETEP during the upgrade process.
- The **show upgrade-status** and **show system-log** CLI commands provide status on the upgrade process. During an upgrade the CLI is available from the serial port, but you cannot initiate an SSH session until the upgrade is complete. The show commands are available in ETEP 1.5 and later.

Related topics:

- [“Log Event Settings” on page 322](#)
- [“Defining Syslog Servers” on page 323](#)

Restoring the Backup File System

The restore operation restores the backup copy of the appliance file system. This operation is available through ETEMS only on ETEP appliances. For other appliance models, use the CLI commands to restore the file system from a backup copy.

As part of the software upgrade process the ETEP preserves a backup copy of the file system. The backup copy of the appliance file system contains a software image, configuration files, policies and keys, certificates, log files, and passwords. Restoring the backup file system replaces the current file system with the backup files.

The restore operation can be reversed. The restore operation essentially toggles between the current file system and the backup image. Each time you issue the restore command, the appliance switches its running image to whichever file system is not currently in use.

Review the following recommendations and cautions prior to restoring the file system:

- Make sure that you know the passwords used in the backup configuration. Once the backup image is restored on the appliance, you must use the passwords from the backup configuration to log in.
- After restoring the file system, redeploy policies to the ETEP using ETPM to ensure that the appliance is using the current set of policies and keys.
- The restore operation replaces the current certificate with the backup certificate. If you replaced a certificate after the backup image was created, you will need to reinstall that certificate after the file system is restored. Failure to do so can result in a communication failure between the ETEP and the ETKMS.

To restore the appliance file system from a backup copy:

- 1 In the Appliance Manager, select the target appliances in the Appliances view.
- 2 On the Tools menu, click **Restore from Backup**. Click **OK** to confirm the action. The appliance will automatically reboot to complete the restore operation.
- 3 Redeploy policies to the ETEP using ETPM to ensure that the appliance uses the current set of policies and keys.

Part III Using ETPM to Create Distributed Key Policies



9

Getting Started with ETPM

The Policy Manager (ETPM) is the security policy management component of the EncrypTight. You use ETPM to create and manage distributed key policies that you send to the Key Management System (ETKMS). The ETKMS generates the keys and distributes the keys and policies to the PEPs.

This section includes the following topics:

- [Opening ETPM](#)
- [About the ETPM User Interface](#)
- [About ETPM Policies](#)
- [Policy Generation and Distribution](#)
- [Creating a Policy: An Overview](#)

Opening ETPM

ETPM is a separate perspective in EncrypTight. You will use both ETEMS and ETPM to manage PEPs, ETKMSs, and policies. Only one instance of ETPM can be used to manage EncrypTight components.

To open ETPM:

- 1 Start EncrypTight.
- 2 Click the **Open Perspective** icon on the top right of the perspective tab and select **Other**, or click **Open** on the **Window** menu and then click **Other**.
- 3 From the Open Perspective window, select **ETPM** and click **OK**.

After you have opened ETPM, you can use the double angle brackets >> on the perspective tab to switch between perspectives.

About the ETPM User Interface

The main ETPM window consists of perspectives, views, editors, a menu, and a tool bar (Figure 42):

- *Perspectives* are used to perform a specific set of tasks
- *Components View* is used to manage the policy components.

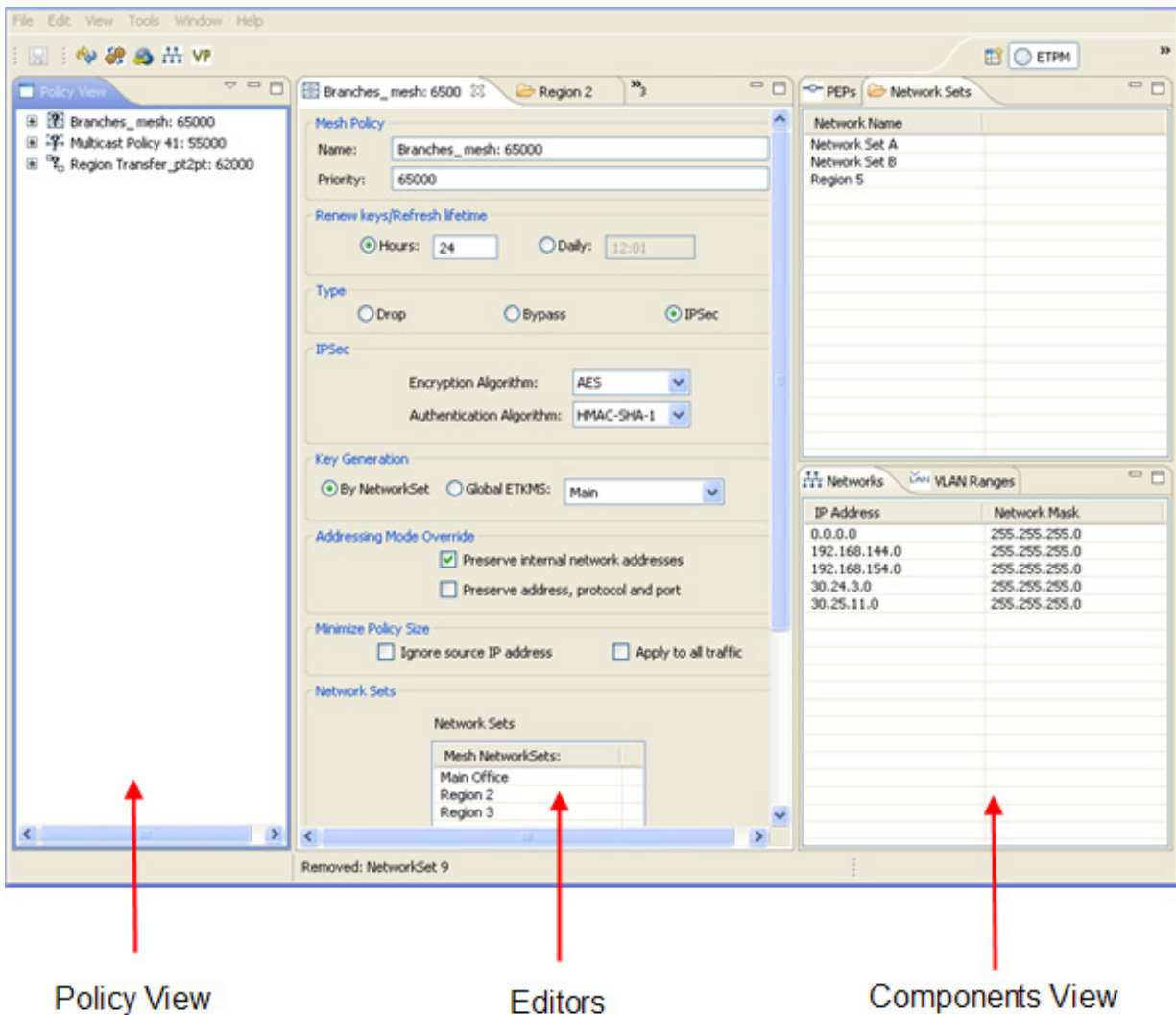
- *Editors* are used to add and modify EncrypTight components and policies.
- *Policy view* is used to view and add policies.

Related topics:

- “EncrypTight Components View” on page 133
- “Editors” on page 134
- “Policy View” on page 135
- “ETPM Toolbar” on page 137
- “ETPM Status Refresh Interval” on page 137

Each of the views can be individually sized by dragging the borders of that area. In addition, each view has three resizing buttons at the top right corner: minimize, maximize and restore. If you right-click on the tab for a view, you can detach the view and drag it to another location on your desktop.

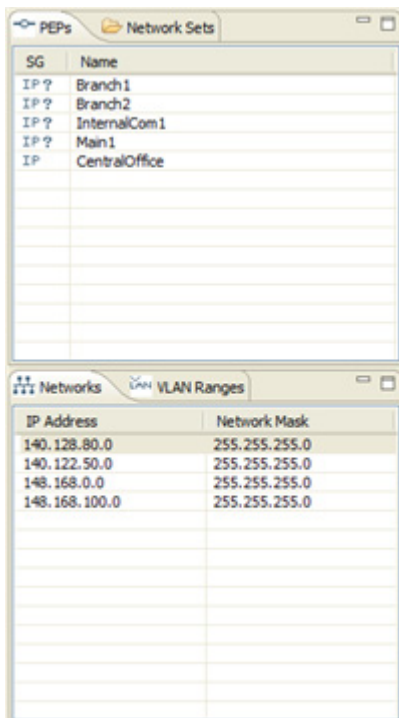
Figure 42 ETPM perspective



EncryptTight Components View

The EncryptTight Components view lets you configure the network components used to create a policy.

Figure 43 EncryptTight Components view



EncryptTight components are the building blocks used to construct a policy. Layer 3 IP policy components are:

- PEPs
- Networks
- Network sets

Layer 2 Ethernet policy components are:

- PEPs
- VLAN ranges

You can sort each of the network component views by clicking column headers. For example, you can sort the networks by clicking the IP address column header.

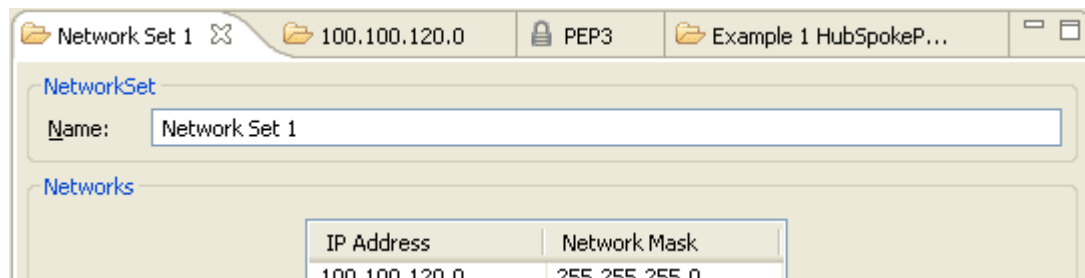
For information on adding, editing, and deleting policy components, refer to the following chapters:

Component	Chapter
PEPs	Chapter 10
ETKMSs	Chapter 11
Networks	Chapter 12
Network Sets	Chapter 13
VLAN Ranges	Chapter 14

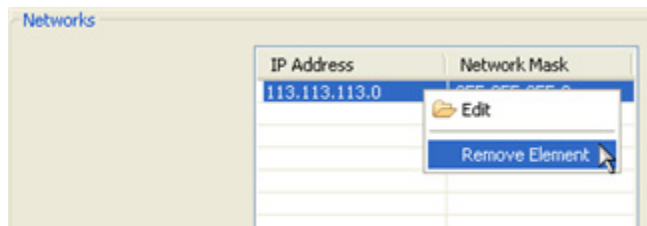
Editors


Editors allow you to add or change EncrypTight components and policies. When you first start ETPM, no editors are open. To open an editor, double-click a component or policy, or right-click and select **Add Element** or **Edit** in the EncrypTight Components view. You can open multiple editors at any time. Each opened editor appears as a tab in the Editors view.

Figure 44 Editors



Some ETPM editors require a drag and drop operation. To enter a PEP, network, network set or VLAN range into an editor, select the appropriate component tab and drag the component to the desired box on the editor. Once the component has been dragged to the editor, the EncrypTight component becomes unavailable in the EncrypTight Components view. To delete components from an editor, right-click on a component in an editor and click **Remove Element**. After you remove a component from an editor, it becomes available again in the EncrypTight Components view.

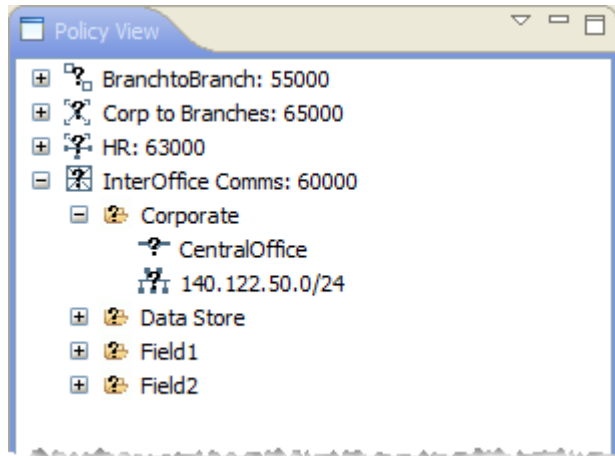


Editors display a  if a policy or EncrypTight component contains a missing or invalid entry. Move the mouse pointer over the error symbol for a tool-tip explanation of the validation problem.

Policy View

The Policy view allows you to view, add, and edit policies.

Figure 45 Policy view



The Policy view lists the policies in an expandable tree structure. You can use the Policy view to add a new policy, edit a policy, and edit or remove any component in a policy. You can expand each policy to view the network sets by clicking the icon. You can further expand the networks sets to view the PEPs and networks included in each network set within that policy.

To edit an element from the policy view:

- 1 Expand the policy to view the desired element within the policy.
- 2 Double-click the element and modify that element in the editor as desired.

In addition to the resizing buttons on the top right of the Policy view, this view has a **Menu** button . The **Menu** button provides four selections:

- **Sort by Name** - sorts the policies by name.
- **Sort by Priority** - sorts the policies by priority.
- **Expand All** - expands all policies listed in the Policy view.
- **Collapse All** - collapses all expanded policies listed in the Policy view.





ETPM Status Indicators

In the Policy view, the status icon shown next to the policy name reflects the overall status of all the components that constitute the policy. To see the status of the individual components, expand the policy tree. [Table 37](#) lists each of the possible status indications.

Table 37 Status indicators

Indication	Legend	Description
	Status Unknown	The current status is unknown or questionable.
	Pending	ETPM performed an action and is waiting for responses from the ETKMSs.

Table 37 Status indicators (continued)

Indication	Legend	Description
	Consistent	ETPM performed an action and the responses from the ETKMSs indicate that the PEPs are consistent with the settings in ETPM.
	Inconsistent	Deployed policies in a PEP do not match the policies in ETPM or no policy is present.
	Communication error	A communication error or timeout has occurred with one or more PEPs included in the policy.
	Configuration error	A configuration error has been detected in one of the policy components.

 **NOTE**

The status indicators displayed in the ETPM Policy view change only after you click *Deploy policies*, *Renew keys*, or *Refresh Status*. The status indicators displayed in the ETEMS Appliance Manager change only after you click *Refresh Status* or *Reload Policies* from the Appliance Manager, and are not affected by the status of the components and policies listed in ETPM Policy view.

Related topic:

- [“Monitoring Status” on page 237](#)

Sorting and Using Drag and Drop

Throughout the ETPM interface you can sort various views and lists by clicking column headings. For example, you can sort the PEPs view by clicking the SG (type) or Name column heading. This functionality is also available within Editors. For example, you can sort the list of Network Sets in the Mesh Policy Editor.







ETPM also makes use of standard Windows selection and drag and drop capabilities. For example, with a mesh policy, you can add a group of network sets in a single step instead of adding individual network sets one at a time. There are two ways to select multiple elements:

- To select a contiguous block of elements, click the first element to select it. Then press and hold the **Shift** key and click the last element in the block.
- To select multiple non-contiguous elements, click the first element to select it. Then press and hold the CTRL key while selecting the other elements.


ETPM Toolbar

The ETPM toolbar provides shortcuts to frequently performed tasks.

Table 38 ETPM toolbar

Button	Description
	Saves the configuration in the active editor.
	imports networks and network sets from a CSV file. For more information on using this feature, see “Importing Networks and Network Sets” on page 172 .
	Refreshes the status of all ETPM components.
	Deploys the ETPM policies. Sends the policy information to the Key Management System for distribution to the PEPs.
	Manually renews the keys for all policies, and refreshes policy lifetimes for Bypass and Drop policies. Renew the keys manually only if you suspect your key security has been compromised, and wait at least 10 minutes before manually renewing keys again. Because the PEP maintains the previous keys for up to five minutes to prevent traffic interruptions, if you renew keys manually the number of keys and security associations (SAs) on each PEP doubles for a period of 5 to 10 minutes.
	Checks your policies for conformance to the policy rules prior to deployment. This tool performs the same consistency checks on policies that are performed during a deploy operation. It differs from the deployment verification in that it does not check communication links to the ETKMS.

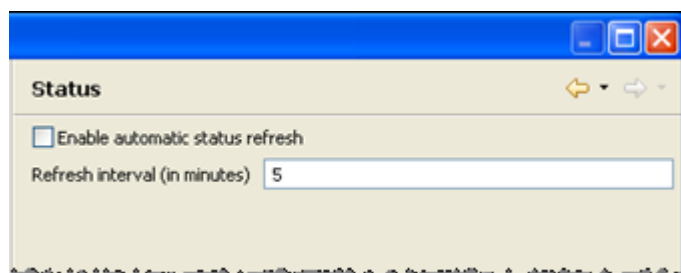
ETPM Status Refresh Interval

By default, automatic status refresh is disabled. You can refresh the status manually by clicking the **Refresh Status**  button. If you prefer, you can have ETPM automatically check the status of the PEPs in deployed policies. The default refresh interval is five minutes and can be changed in one minute increments from 1 to 60 minutes.

To enable or disable automatic status checking:

- 1 From the ETPM main menu bar, click **Edit > Preferences**.
- 2 In the Preferences window, expand the ETPM listing and select **Status**.

Figure 46 ETPM Preferences



- 3 Click **Enable automatic status refresh** to have ETPM automatically check the status of the **PEPs**, or clear the check box to turn off the feature.
- 4 If you enabled automatic status checking, enter the interval in minutes in the **Refresh Interval** box.
- 5 Click **Apply**.

About ETPM Policies

A policy specifies what traffic to protect and how to protect it. Each packet or frame is inspected by the PEP and processed based on the filtering criteria specified in the policy. Each policy specifies:

- The PEPs to be used
- The ETKMSs to be used
- The networks the PEPs will protect
- The action that is to be performed (encrypt, send in the clear, or drop)
- The kind of traffic the policy affects

Filtering criteria can be high level, such as “encrypt everything,” or more granular, specifying traffic based on IP addresses, protocols, or VLAN ranges. After applying the traffic filters, the PEP takes one of three actions: it encrypts the packet (IPSec), passes it in the clear (bypass), or it drops the packet.

Related topics:

- [“IP Policies” on page 138](#)
- [“Ethernet Policies” on page 138](#)

IP Policies

EncryptTight supports policies for Layer 2 Ethernet networks and Layer 3 IP networks, based on the type of PEPs used for encryption. Supported IP topologies are:

- Hub and spoke
- Mesh
- Point-to-point
- Multicast

Layer 3 IP policies protect IP traffic using ETEP PEPs.

IP policies consist of four components:

- ETEP PEPs enforce the policies
- ETKMSs distribute the keys and policies to the PEPs
- Networks identify the IP addresses of the networks included in the policy
- Network Sets associate the networks to the protecting PEPs and the supporting ETKMS

Ethernet Policies

In Layer 2 Ethernet, the supported topology is meshed networks. If an Ethernet network uses VLAN ID tags, a virtual point-to-point topology can be established.

Layer 2 Ethernet policies protect Ethernet traffic using ETEP PEPs. An Ethernet policy can be applied to all Layer 2 traffic or restricted to traffic that contains VLAN ID tags that fall within a given range. Ethernet policies consist of three components:

- ETEP PEPs enforce the policies

- ETKMSs distribute the keys and policies to the PEPs
- VLAN ID ranges enable filtering based on VLAN ID tags (optional)

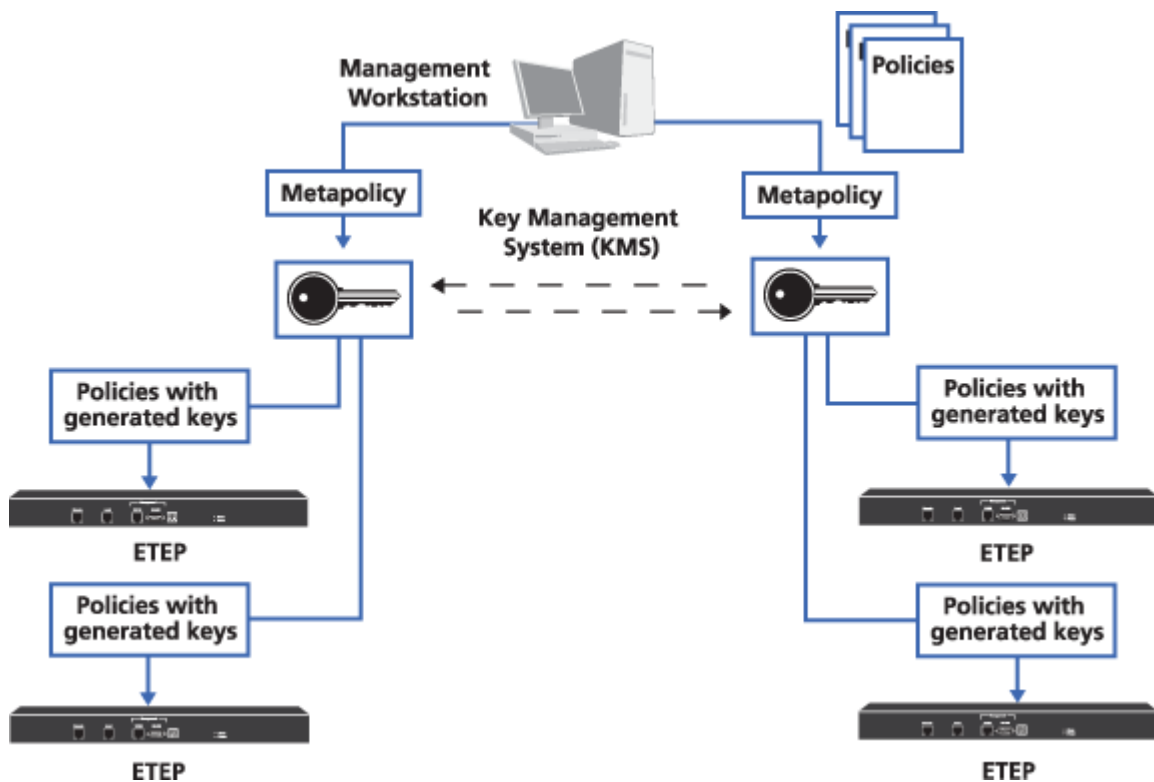
 **NOTE**

If you do not include a VLAN ID or range in the policy, all Ethernet traffic is selected for enforcement.

Policy Generation and Distribution

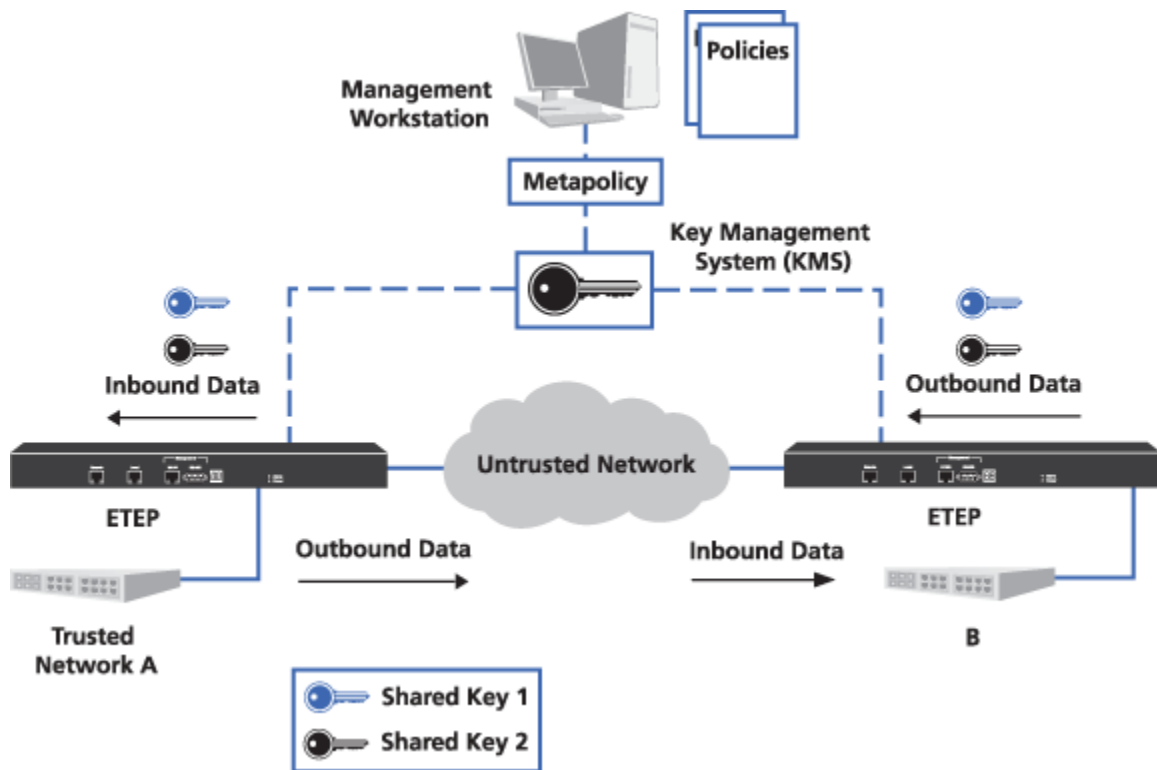
This section outlines how the elements of EncrypTight work together to generate and distribute policies and keys. While an actual deployment might be significantly more involved than the examples used, the concepts remain the same. [Figure 47](#) illustrates the basic generation and distribution of policies and keys within EncrypTight.

Figure 47 Policy generation and distribution



When you deploy the policies, the ETPM sends a metapolicy to each ETKMS. The metapolicy contains all of the information regarding each policy including the action (encrypt, clear, or drop), the required ETKMSs, the lifetime of the policy, the PEPs that enforce the policies, and what kind of traffic the policy acts on. Each ETKMS generates the required keys and sends the appropriate policies along with the shared keys to each of its PEPs.

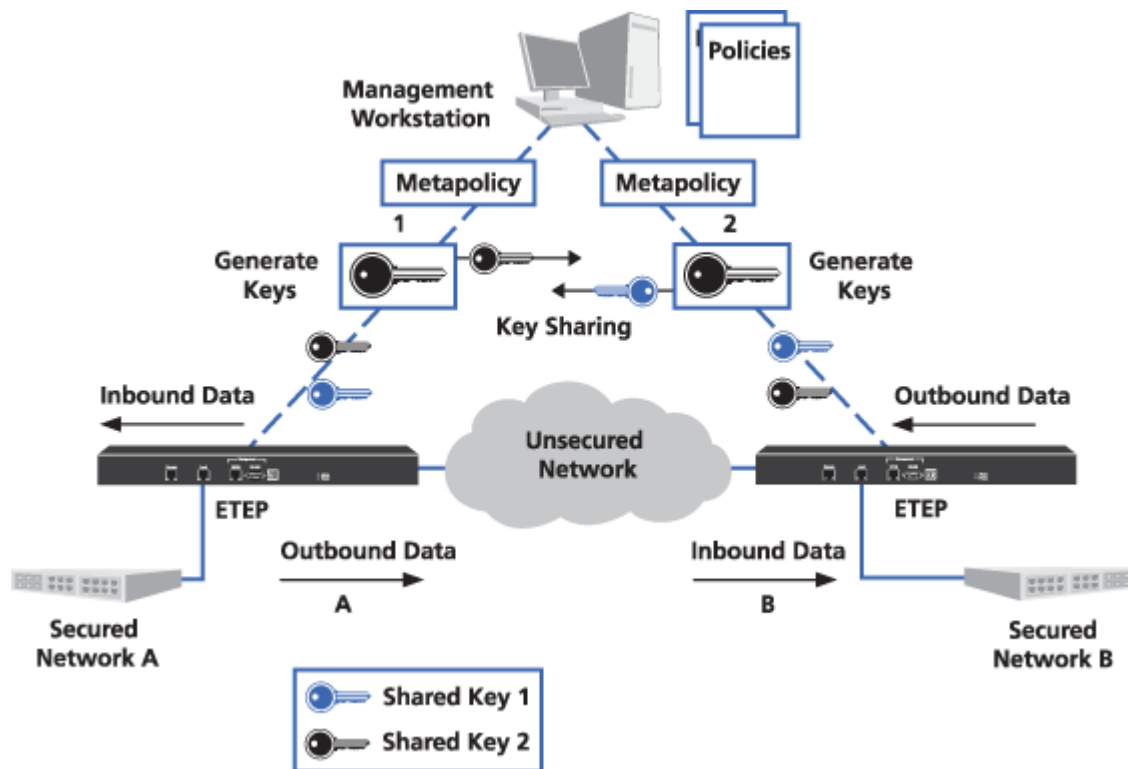
When two or more PEPs are controlled by the same ETKMS, that ETKMS generates the shared keys for the PEPs. [Figure 48](#) illustrates key generation and distribution when one ETKMS controls multiple PEPs required to enforce an encryption policy.

Figure 48 Key generation with one ETKMS

In this scenario, you could use either a local ETKMS or an external ETKMS. The ETKMS generates and sends the same shared key to the PEP encrypting the outbound data and the PEP decrypting the inbound data. Each PEP needs a unique key to encrypt outbound data, and in turn this key must be shared with the PEP's peers.

- In [Figure 48](#), the ETKMS generates Shared Key 1 and distributes this key to PEP B to encrypt the outbound data and to PEP A to decrypt the inbound data.
- The ETKMS also generates Shared Key 2 and distributes this key to PEP A to encrypt the outbound data from Network A and to PEP B to decrypt the inbound data to Network B.

A policy can use two or more PEPs that are controlled by different ETKMSs. In this case, first the controlling ETKMSs exchange the keys PEPs need for decrypting traffic and then they send the appropriate keys to the PEPs they control. [Figure 49](#) illustrates key generation and distribution when different ETKMSs control the PEPs required to enforce an encryption policy. This scenario would most likely involve two external ETKMSs.

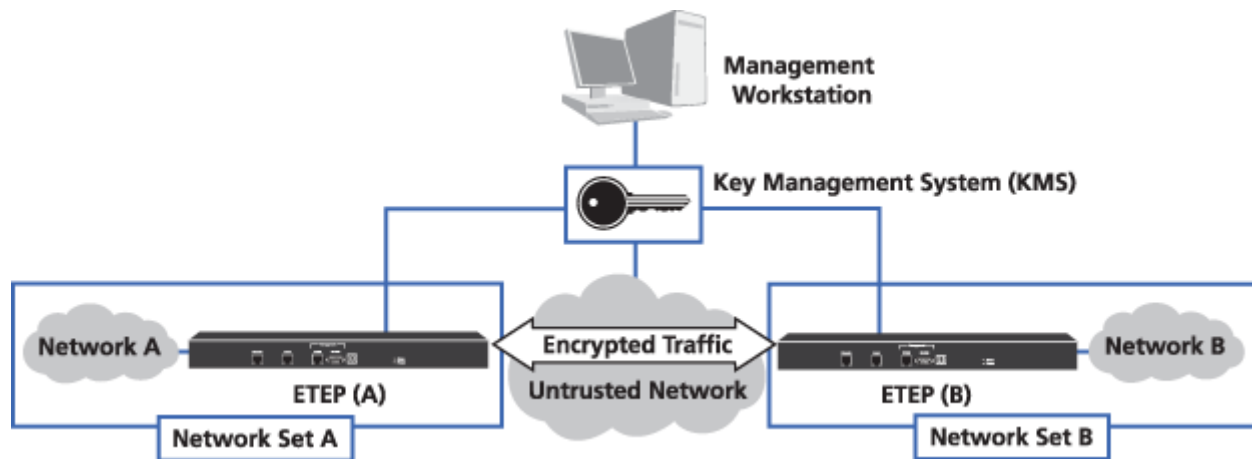
Figure 49 Key generation with multiple ETKMSs

The ETKMS generating the key for a PEP's outbound data shares the key with the ETKMSs that control the PEPs that decrypt the data. In [Figure 49](#), ETKMS 1 controls PEP A and is responsible for generating Shared Key 2. ETKMS 2 controls PEP B and is responsible for generating Shared Key 1.

- Shared Key 2 is used to encrypt the outbound data in PEP A and it is used by PEP B to decrypt the data received from Network A. ETKMS 1 shares Shared Key 2 with ETKMS 2, which distributes the key to PEP B.
- Shared Key 1 is used to encrypt the outbound data from PEP B and it is used by PEP A to decrypt the data received from Network B. ETKMS 2 shares Shared Key 1 with ETKMS 1, which distributes the key to PEP A.

Creating a Policy: An Overview

The following steps summarize how to create a point-to-point IP policy, using the example in [Figure 50](#). If you are configuring a policy for a Layer 2 Ethernet network the overall procedure is the same but the specific components are different.

Figure 50 Sample point-to-point IP policy

Elements of [Figure 50](#):

1)	ETKMS 1, IP address 192.168.1.33
A, B)	PEP A, IP address 192.168.11.69 PEP B, IP address 192.168.11.224
Network A	IP address 192.168.144.0
Network B	IP address 192.168.154.0
Network Set A	Includes Network A and PEP A, using ETKMS 1
Network Set B	Includes Network B and PEP B, using ETKMS 1

[Figure 50](#) illustrates an EncrypTight deployment with two networks. This example demonstrates how to create a point-to-point policy to encrypt the traffic sent between the two networks over the untrusted network.

To create a policy, the general steps are:

- 1 In the ETEMS Appliance Manager,
 - a Add and configure the PEPs you want to use.
 - b Push the configurations to the PEPs.
 - c Add and configure the ETKMSs you want to use.
- 2 In ETPM,
 - a Add the networks you need.
 - b Create the network sets.
 - c Create the policies.
 - d Deploy the policies.

To create a policy:

- 1 In the ETEMS Appliance Manager, add PEP A and PEP B (**File > New Appliance**).

In the sample illustrated in [Figure 50](#), the management port of PEP A has the IP address 192.168.11.69 and the management port of PEP B has the IP address 192.168.11.224.

To use an appliance as an EncrypTight PEP, you need to click the **Enable EncrypTight** setting on the **Features** tab of the New Appliance editor. Other settings are also strongly recommended, as discussed in [“Adding a New PEP in ETEMS”](#) on page 148.

 **NOTE**

Although you can create networks and other elements in ETPM, no ETPM data is saved until you add at least one PEP in the ETEMS Appliance Manager.

- 2 In the Appliance Manager, select PEP A and PEP B and push the configurations to the PEPs (**Tools > Put Configurations**). A reboot is not required for ETEP PEPs.

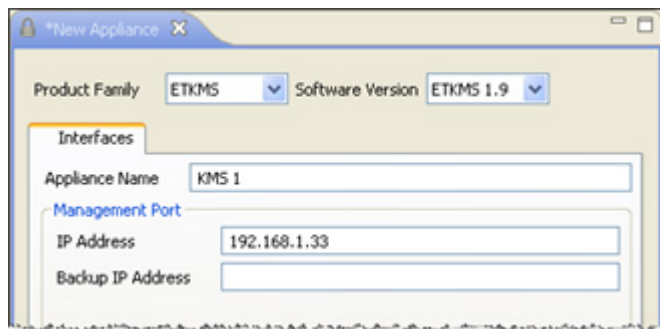
Name	Management IP	Result
PEP B	192.168.11.224	pending
PEP A	192.168.11.69	pending


Reboot appliances immediately after operations complete

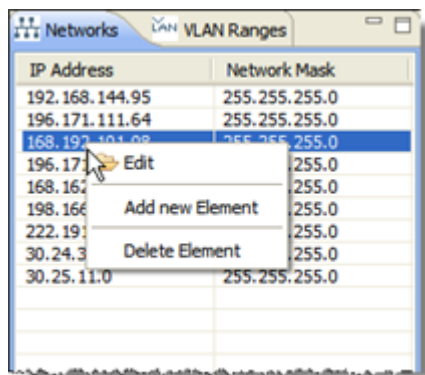
Put Close

- 3 In the Appliance Manager, add and configure ETKMS 1 (**File > New Appliance**).

In the sample illustrated in [Figure 50](#), ETKMS 1 has the IP address 192.168.1.33 and does not have a backup ETKMS.



- 4 In the Appliances view, select ETKMS 1 and click **Refresh Status** . For more information, see [“Adding ETKMSs” on page 156](#). This helps you determine that the ETKMS is accessible and operating properly.
- 5 Start ETPM. Click the **Open Perspective** button on the perspective tab and select **Other**. From the Open Perspective window, select **ETPM** and click **OK**.
- 6 In the ETPM window, click the **Networks** tab and add Network A and Network B.



In the sample illustrated in [Figure 50](#), Network A has the IP address 192.168.144.0 and Network B has the IP address 192.168.154.0. For more information, see [“Adding Networks” on page 159](#).

- 7 Click the **Network Sets** tab and in the editor, add Network Set A and Network Set B.



In the sample illustrated in [Figure 50](#), Network Set A includes Network A and PEP A, and uses ETKMS 1. Network Set B includes Network B and PEP B, and uses ETKMS 1. For more information about Network Sets, see [“Adding a Network Set” on page 170](#).

- 8 Right-click in the **Policy** view tab and select **Add Point-to-Point Policy**. A New Point-to-Point Policy editor opens.

- Click the **New Point-to-Point Policy** editor and configure a point-to-point IPSec policy using the components you created in the preceding steps. See [“Adding Layer 3 IP Policies” on page 191](#) for more information.

The screenshot shows the configuration interface for a Point-to-Point Policy. The window title is "Region Transfer: 62000". The configuration is as follows:

- Name:** Region Transfer: 62000
- Priority:** 62000
- Renew keys/Refresh lifetime:** Hours: 24 (selected), Daily: 12:01
- Type:** Drop, Bypass, IPSec (selected)
- IPSec:** Encryption Algorithm: AES, Authentication Algorithm: HMAC-SHA-1
- Key Generation:** By NetworkSet (selected), Global ETKMS: [dropdown]
- Addressing Mode Override:** Preserve internal network addresses (checked), Preserve address, protocol and port (unchecked)
- Minimize Policy Size:** Minimize Policy Size (ignore source IP address) (unchecked)
- Network Set Point A:** Point A, NetworkSet: Network Set A, Source Port: Any Port (selected), Only Port: 0, Dest Port: Any Port (selected), Only Port: 0
- Network Set Point B:** Point B, NetworkSet: Network Set B, Source Port: Any Port (selected), Only Port: 0, Dest Port: Any Port (selected), Only Port: 0

To create a policy for the sample illustrated in [Figure 50](#), click and drag Network Set A to the Point A box and Network Set B to the Point B box. For information on other settings you can specify for policies, see [“Policy Concepts” on page 181](#).

- Deploy the policies to the ETKMSs and PEPs (**Tools > Deploy**).

10 Managing Policy Enforcement Points

Policy Enforcement Points (PEPs) enforce the policies created in ETPM and distributed by the ETKMSs. EncrypTight Policy Enforcement Points (ETEP PEPs) include:

- ET0010A
- ET0100A
- ET1000A

This section includes the following topics:

- [Provisioning PEPs](#)
- [Editing PEPs](#)
- [Deleting PEPs](#)

Provisioning PEPs

Provisioning PEPs requires adding and configuring an appliance and then pushing the configuration to the appliance.

Related topics:

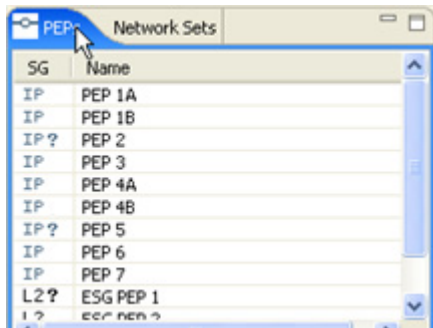
- [“Adding a New Appliance” on page 147](#)
- [“Adding Large Numbers of PEPs” on page 150](#)
- [“Pushing the Configuration” on page 151](#)
- [“Provisioning Basics” on page 95](#)

Adding a New Appliance

You can add a new appliance to be used as an EncrypTight PEP from the ETEMS Appliance Manager or ETPM. To simplify the provisioning process, we recommend adding all PEPs from the ETEMS. If you add a PEP from ETPM, you will have to switch to the ETEMS Appliance Manager to push the configuration to the appliance.

The EncrypTight Components view of ETPM shows a list of available appliances under the PEPs tab. PEPs shown in the PEPs view are designated by type: IP or L2 (Ethernet). IP PEPs can be used in the

network sets in Layer 3 IP policies. L2 PEPs can be used in Layer 2 Ethernet policies. You can sort the list of PEPs by type or name by clicking the column header (SG or Name).



When ETEMS communicates with a PEP, it verifies that its hardware and software configuration is valid. PEPs that ETEMS has not yet communicated with are marked with a ? symbol beside the IP or L2 designation. In the previous example, PEP 2, PEP 5, and ESG PEP 1 have not yet had any communications from ETEMS. Once you refresh the status or push configurations from ETEMS, the ? symbol disappears. The first time you attempt to use a PEP with the ? symbol, the following warning appears.



Related topics:

- [“Adding a New PEP in ETEMS” on page 148](#)
- [“Adding a New PEP Using ETPM” on page 150](#)

Adding a New PEP in ETEMS

It is recommended that you add all new PEPs in the ETEMS Appliance Manager because you can only push configurations to the PEPs in ETEMS. All appliances used as EncrypTight PEPs must have the configuration settings described in [Table 39](#).

Table 39 EncrypTight PEP configuration

Configuration	Description
Network interfaces	On the Interfaces tab, configure the PEP’s management, local, and remote ports. If the PEP and the ETKMS are on different subnets, specify a default gateway for the management port that the PEP can use for communication with the ETKMS and the management workstation hosting ETPM.

Table 39 EncryptTight PEP configuration (continued)

Configuration	Description
Enable EncryptTight	<p>On the Features tab, select Enable EncryptTight. EncryptTight is enabled by default on ETEP PEPs.</p> <p>After you enable EncryptTight, the default behavior of all PEPs is to send all packets in the clear until you deploy new policies. Once you deploy policies, the PEPs process traffic as directed by the policies.</p>
Enable passing TLS traffic in the clear	<p>For all PEPs that pass TLS traffic between the ETPM and ETKMSs and between the ETKMSs and PEPs, enable passing TLS traffic in the clear. If this is not enabled, any ETPM to ETKMS, or ETKMS to PEP communications will not pass through this PEP.</p> <ul style="list-style-type: none"> On the Features tab, select Enable passing TLS traffic in the clear. This is the default setting when EncryptTight is enabled.
Encryption Policy Settings (ETEP only)	<p>On the Features tab, specify whether you want the ETEP PEP to operate as a Layer 2 (Ethernet) PEP or a Layer 3 (IP) PEP.</p>
Enable the SNTP client for time synchronization	<p>If you enable an SNTP client on the PEP, provide a server address for the most reliable source that retrieves time from a stratum 3 or higher clock source. If the EncryptTight components are not synchronized with a reliable clock source and the time difference between components is significant, policies and keys can expire before they would normally be renewed. Traffic can get dropped or mistakenly passed in the clear.</p> <ul style="list-style-type: none"> On the Advanced tab, select Enable SNTP Client. Enter the IP address of the NTP service. .
Other configuration settings	<p>For complete information about appliance configuration, refer to “Provisioning Appliances” on page 95 and the configuration chapter for the PEP that you are using.</p>

 **NOTE**

- For more information about PEP configuration options, see the chapter for the PEP model that you are using.
- Although you can create networks and other elements in ETPM, no ETPM data is saved until you add at least one PEP in the ETEMS Appliance Manager.
- If you re-provision a PEP that has been out of service, it is recommended that you synchronize the appliance with an NTP server and reboot it before you attempt to use the PEP with either ETEMS or ETPM. For more information see [“Network Clock Synchronization” on page 33](#).

Related topics:

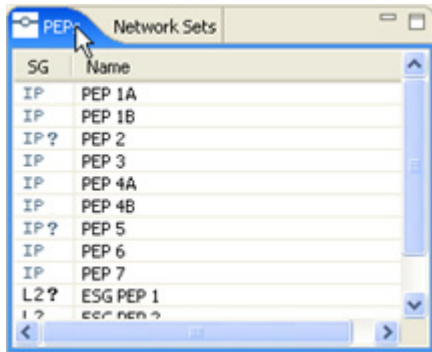
- [“Provisioning Basics” on page 95](#)
- [“ETEP Configuration” on page 299](#)

Adding a New PEP Using ETPM

Normally, you should add PEPs using the ETEMS Appliance Manager; however, it is possible to add PEPs from ETPM. Keep in mind that you will have to use ETEMS to push the configurations to the PEPs.

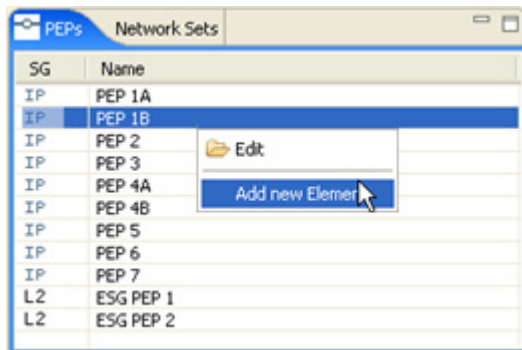
To add a new PEP using ETPM:

- 1 From the EncrypTight Components view on ETPM, click the PEPs tab.



The PEP tab displays a list of all configured PEPs.

- 2 Right-click anywhere in the PEP view and then click **Add new Element**.



- 3 Enter the PEP's properties on the appliance editor as required by your network configuration. Refer to [Table 39](#).
- 4 Click **Save** when complete.

Adding Large Numbers of PEPs

When you have a large number of PEPs to add, entering each configuration individually is time-consuming. To minimize the time needed to add and configure new PEPs, create customized default configurations for your PEPs and use the Import Configurations feature in ETEMS to import basic appliance information for a large number of appliances from a .csv file.

In the customized default configurations, make sure to specify the settings critical to EncrypTight, as outlined in [Table 39](#).

Related topics:

- [“Working with Default Configurations” on page 110](#)
- [“Provisioning Large Numbers of Appliances” on page 111](#)

Pushing the Configuration

After you define the PEP configurations, push the configurations from ETEMS to the targeted PEPs.

To push ETEMS configurations to PEPs:

- 1 In the ETEMS Appliances view, select the target PEPs.
- 2 On the **Tools** menu, click **Put Configurations**.
- 3 Some appliance models must be rebooted for configuration changes to take effect. Rebooting interrupts the data traffic on the PEP's remote and local ports for several minutes. To reboot the PEP immediately following a successful put operation, click the **Reboot appliances after operations complete** check box on the Put Configurations window. Clear the check box to reboot at a later time.
- 4 In the Put Configurations window, click **Put** to push configurations.
- 5 Click **Close** to return to the Appliances view, and then refresh the appliance status (**Tools > Refresh Status**). If you chose to reboot the PEPs after loading the configurations, wait a few minutes for the reboot operation to complete before refreshing the status.

Related topic:

- [“Pushing Configurations to Appliances” on page 97](#)

Editing PEPs

PEP configurations can be edited from ETEMS or ETPM. To simplify the editing process, we recommend editing all PEPs from ETEMS, where you can edit configurations and push them to the PEPs. If you edit a PEP from ETPM, you will have to switch to ETEMS to push the modified configuration to the PEP.

Related topics:

- [“Editing PEPs From ETEMS” on page 151](#)
- [“Editing Multiple PEPs” on page 152](#)
- [“Editing PEPs From ETPM” on page 152](#)
- [“Changing the IP Address of a PEP” on page 153](#)

Editing PEPs From ETEMS

To edit a PEP's configuration:

- 1 In the ETEMS Appliances view, select the PEP.
- 2 On the **Edit** menu, click **Configuration**.
- 3 In the appliance editor, modify the configuration. Refer to [Table 39](#). To change all of the values to their defaults, click **Use Defaults**.
- 4 When you are done, click **OK**. The modified configuration is saved for subsequent downloading to the PEP.
- 5 For the new configuration to take affect in the PEP, you must push the configuration to the PEP. In addition, some changes might require you to reboot the PEP.

If you changed the PEP's Appliance name in ETEMS, redeploy your policies. If you don't redeploy, the renamed PEP will issue an error message after every key refresh.

Related topic:

- [“Pushing Configurations to Appliances” on page 97](#)

Editing Multiple PEPs

Changing the configurations of a large number of PEPs can be time-consuming. However, there are specific settings that you can change for a selection of multiple PEPs. For EncrypTight users, the most significant of these is the preferred NTP server. For information on other settings that you can modify for a selection of multiple PEPs, see [“Changing Settings on Multiple Appliances” on page 121](#).

To change the NTP settings for multiple PEPs:

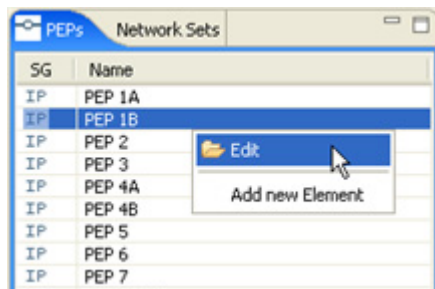
- 1 In the ETEMS Appliance Manager, select the PEPs that you want to change. You can select a mix of different types of PEPs.
- 2 Select **Edit > Multiple Configurations > SNTP Client**.
- 3 To change the NTP server, click **Enable**, enter the address in the **IP Address** box, and click **Apply**.
- 4 Push the new configuration to the PEPs.

Editing PEPs From ETPM

Normally, you should edit PEPs using ETEMS; however, for convenience you can edit PEPs from ETPM. Keep in mind that you will have to use ETEMS to push the configurations to the PEPs.

To modify an existing PEP from ETPM:

- 1 In the EncrypTight Components view of ETPM, click the PEPs tab.
- 2 Right-click the desired PEP click **Edit**.



- 3 Change the entries of the desired fields in the editor.
- 4 Click **Save** when all entries are modified as desired.
- 5 For the new configuration to take affect in the PEP, you must push the configuration to the PEP. In addition, some changes might require you to reboot the PEP.

If you changed the PEP's Appliance name, you will need to redeploy your policies. If you don't redeploy, the renamed PEP will issue an error message after every key refresh.

Related topic:

- [“Pushing the Configuration” on page 151](#)

Changing the IP Address of a PEP

Occasionally, you might need to change the IP address on a PEP. For example, you might need to move a PEP from one location in your network to another. This could require that you change the management IP address of the PEP.

Although you can edit the IP address of a PEP in ETEMS, ETPM and the ETKMSs will not immediately be aware of the change. Any policies currently on the PEP will eventually expire and will not get new keys or be renewed. This causes rekey failures and can lead to a loss of network traffic.

To change the IP address of a PEP:

- 1 In ETPM, temporarily remove the PEP from the policies in which it is used and redeploy those policies.
- 2 In ETEMS, change the IP address of the PEP.
- 3 In ETPM, re-add the PEP to the policies or create new policies and redeploy.

Changing the PEP from Layer 3 to Layer 2 Encryption

The Encryption Policy Setting determines the type of policies that the ETEP PEP can be used in when you create policies in ETPM: Layer 2 Ethernet policies or Layer 3 IP policies. Appliances that are configured for Layer 2 cannot be used in Layer 3 policies, and vice versa.

You can change the ETEP's Encryption Policy Setting on the Features tab of the ETEMS Appliance editor. When you change the encryption policy setting of an in-service ETEP PEP, all encrypt and drop policies currently installed on the PEP are removed and all traffic is sent in the clear until you create and deploy new policies.

Related topics:

- [“Features Configuration” on page 330](#)
- [“Encryption Policy Settings” on page 334](#)

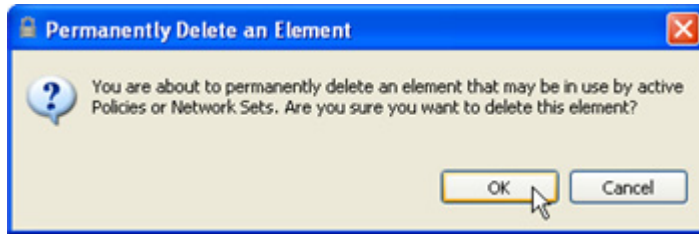
Deleting PEPs


Occasionally, you might need to delete a PEP from ETEMS. For example, the structure of a network might change or a PEP might become redundant. If you are removing a PEP from service, delete the PEP from ETEMS and then deploy policies from ETPM before physically removing the PEP from service.

If you delete a PEP from ETEMS, it is removed from the EncrypTight workspace, and in ETPM it is automatically removed from any network set or policies that include that PEP. Until you redeploy policies, the ETKMS does not know that the PEP has been removed and it continues to renew the keys and lifetimes in the PEP. The PEP itself continues to execute the policies. When you deploy your policies, the ETKMS sends a message to the PEP that instructs it to discard all of the policies from that ETKMS.

To delete PEPs:

- 1 In the Appliances view in ETEMS, select the PEPs to delete.
- 2 On the **Edit** menu, click **Delete**. A confirmation message displays.



- 3 Click **OK**.
- 4 From ETPM, click **Deploy**  .

11 Managing Key Management Systems

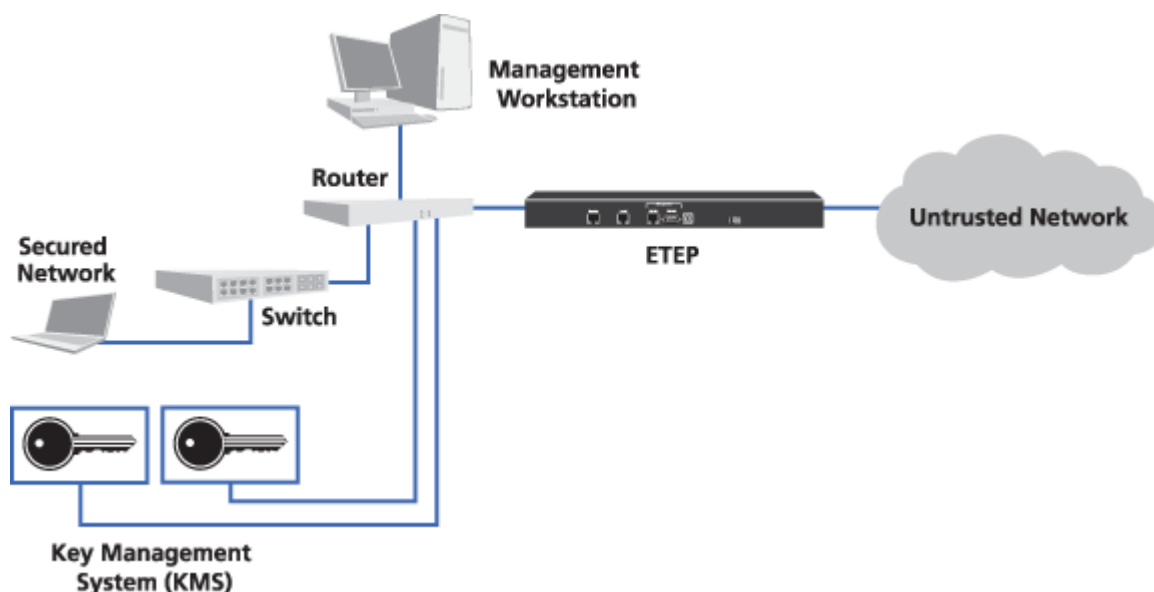
Based on the policies received from the ETPM, the Key Management Systems (ETKMSs) generate and distribute the keys along with the policies to the Policy Enforcement Points (PEPs). You must use the ETEMS Appliance Manager to add, edit, and delete ETKMSs.

This section includes the following topics:

- Adding ETKMSs
- Editing ETKMSs
- Deleting ETKMSs

To add a ETKMS to ETEMS, you need to know the IP address that was assigned to the management port during the installation of the ETKMS. The management port is one of the Ethernet ports (normally GB1). For information about ETKMS installation, refer to “[Configuring ETKMSs](#)” on page 43.

Figure 51 ETKMS connections



Depending on the size and configuration of the network, the EncrypTight system may use one or more ETKMSs distributed throughout the network. EncrypTight also includes a local ETKMS that runs as a separate application on the same management workstation as the EncrypTight software. Local ETKMSs are intended for small to medium networks with no more than 10 nodes.

In order to ensure network resiliency, some EncrypTight configurations may have external ETKMSs installed in pairs: a primary ETKMS and a backup ETKMS. The ETPM distributes the policies to both the primary ETKMS and backup ETKMS. Only the primary ETKMS distributes the keys and policies to the PEPs. If a communication failure occurs with the primary ETKMS due to a ETKMS failure or network failure, the backup ETKMS assumes the generation and distribution of the keys and policies to the PEPs. Once communication with the primary ETKMS is reestablished, the primary resumes the distribution of the keys and policies to the PEPs.

 **CAUTION**

Do not add backup ETKMSs as separate appliances in the Appliance Manager in ETEMS. Backup ETKMSs should only be specified in the Backup IP Address box in the ETKMS editor. Backup ETKMSs are not listed in the Appliance Manager view. If you add a backup ETKMS to the Appliance Manager, you can accidentally use it in network sets and policies, which will interfere with the ability of the server to act as a backup.

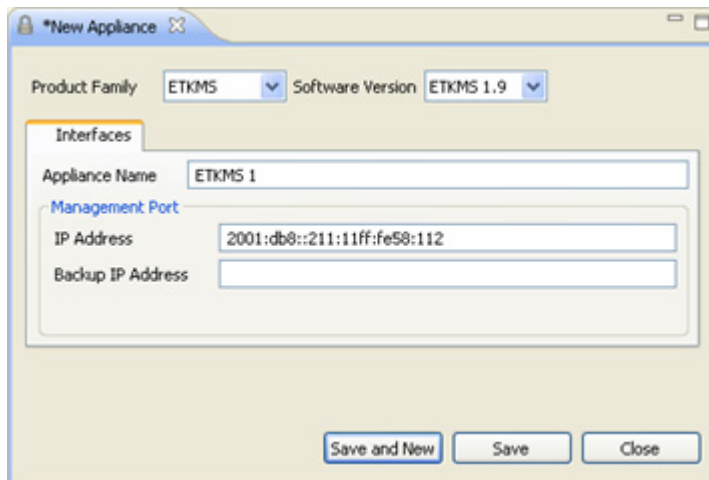
Adding ETKMSs

To add an ETKMS:

- 1 From the perspective tab, click >> and select **Appliance Manager**.
- 2 In the Appliance Manager, select **File > New Appliance**.
- 3 Select **Product Family > ETKMS** and **Software Version ETKMS n.n** where *n.n* is the appropriate ETKMS version.

If you want to add a local ETKMS, select **ETKMS LM** and the appropriate software version. Enter the ETKMS properties in the ETKMS appliance editor as described in [Table 40](#).

Figure 52 Key Management System appliance editor



4 Click **Save** when complete.

Table 40 ETKMS entries

Field	Description
Appliance Name	<p>Enter a unique name to identify this particular ETKMS in the Appliance Name edit box.</p> <p>With external ETKMSs, this name must match the short hostname that was set when the ETKMS was installed and configured. For example, if the hostname was etkms1.mycompany.com, the short hostname is etkms1. Names can be 1 - 40 characters in length. Alphanumeric characters and spaces are valid. The special characters <, >, &, " * , ? , / , \ , : and cannot be used in the ETKMS name. Names are case sensitive.</p>
Management Port IP Address	<p>Enter the IP address of the ETKMS. You can use either an IPv4 or an IPv6 IP address.</p> <ul style="list-style-type: none"> For external ETKMSs, use the same IP address that was assigned to the ETKMS management port when the ETKMS was installed and configured. For local ETKMSs, enter the appropriate IP address. In many cases, this will be the IP address of the management workstation on which the EncryptTight software is installed. <p>For more information on installing and configuring a ETKMS, see “Configuring ETKMSs” on page 43.</p>
Management Port Backup IP Address	<p>Enter the IP address of the backup ETKMS. The IP address was assigned to the ETKMS management port when the ETKMS was installed and configured.</p> <p>Backup ETKMSs must use the same type of address as the primary ETKMS. For example, if the primary uses an IPv6 address, the backup must use an IPv6 address.</p> <p>This entry is only required when a backup ETKMS is used.</p>

Editing ETKMSs

If you change the name or the IP address of a local ETKMS, stop the local ETKMS software and restart it for the changes to take effect (see [“Launching and Stopping a Local ETKMS” on page 45](#)). For external ETKMSs, stop and restart the ETKMS service (see [“Starting and Stopping the ETKMS Service” on page 53](#)).

To edit an existing ETKMS:

- 1 From the ETEMS Appliances view, select the ETKMS.
- 2 On the **Edit** menu, click **Configuration**.
- 3 Change the entries of the desired fields in the editor. [Table 40](#) describes the entries in the ETKMS editor.
- 4 Click **Save** when all entries are modified as desired.

Deleting ETKMSs

Occasionally, you might need to delete a ETKMS. For example, if the structure of a network changes, you might want to delete a ETKMS, and then relocate and reconfigure it.

 **CAUTION**

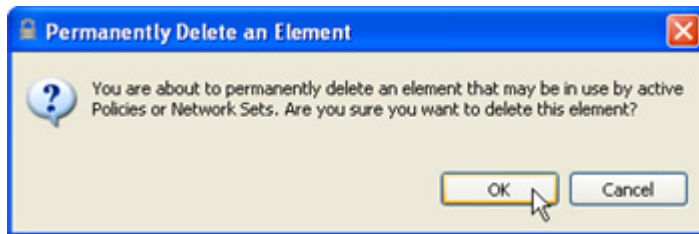
*Do not delete any ETKMSs currently used by any network sets or policies. Before you delete a ETKMS, modify any network sets and policies using that ETKMS to use another ETKMS. If you delete a ETKMS that is currently used in a policy or a network set, you can create configuration errors that might prevent you from deploying your policies. In this case, check the Policy view to find the components with configuration errors. Correct the errors and then click **Deploy**.*

 **CAUTION**

After you remove a ETKMS from network sets and policies, deploy the changed policies. The deploy action sends a policy with no active components to all unused ETKMSs. This policy tells the ETKMS to stop executing all ETPM activity. The ETKMS then sends a message to the PEPs to remove its policies. If you do not deploy before you delete the ETKMS from ETEMS, the old policies remain on the ETKMS. The ETKMS will continue to issue keys and renew policy lifetimes based on the old policies that included that ETKMS. This can cause unexpected dropped or unencrypted traffic.

To delete an existing ETKMS:

- 1 Prior to deleting any ETKMSs, modify any network sets and policies using that ETKMS to use another ETKMS.
- 2 Once the network sets and policies have been modified, click **Tools > Deploy**.
- 3 In the Appliances view in *ETEMS*, select the ETKMS to delete.
- 4 On the **Edit** menu, click **Delete**. A confirmation message displays.



- 5 Click **OK**.

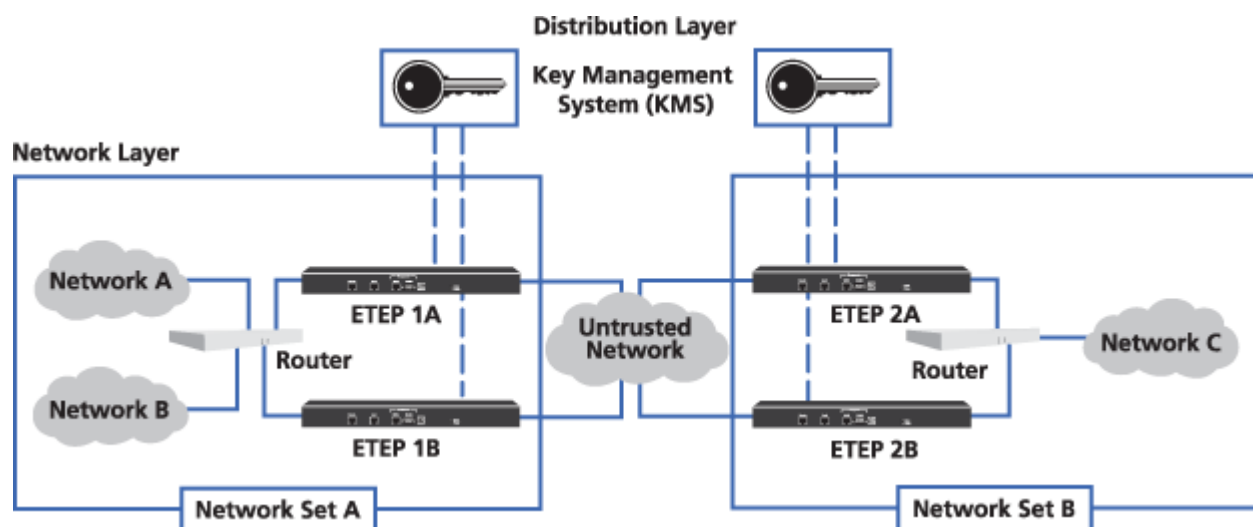
12 Managing IP Networks

In EncryptTight, networks are the IP networks that you want to protect. One or more of these networks are combined with one or more PEPs to make a network set. Network sets are treated as a single network entity within IP policies. Networks are added, modified, and deleted using the networks tab in the EncryptTight Components view.

This section includes the following topics:

- [Adding Networks](#)
- [Advanced Uses for Networks in Policies](#)
- [Editing Networks](#)
- [Deleting Networks](#)

Figure 53 Networks used in a network set

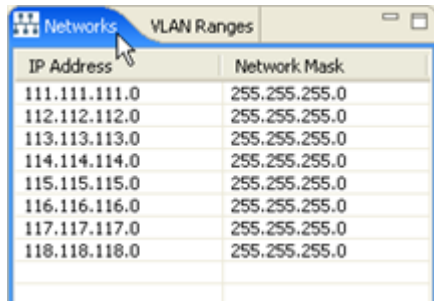


Adding Networks

When you add networks, you need to know the IP address and subnet mask of each network. If you have a large number of networks to add, you can import a list from a CSV file. For more information, see [“Importing Networks and Network Sets”](#) on page 172.

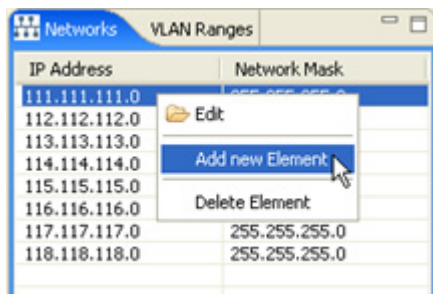
To add a network:

- 1 From the EncryptTight Components view, click the **Networks** tab.



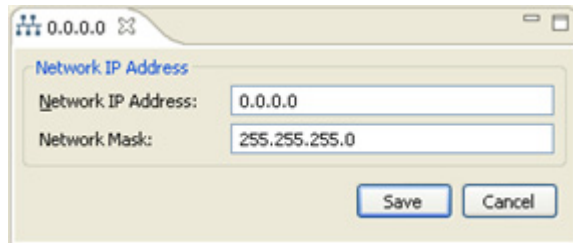
The Networks tab lists all of the networks that have been added. You can sort of the list of networks by IP address or network mask by clicking a column header.

- 2 Right-click anywhere in the Networks tab and click **Add new Element**.



- 3 Create the network in the Network editor as described in [Table 41](#). Enter the IP address and subnet mask to select the traffic of interest.

Figure 54 Network editor



- 4 Click **Save** when complete.

Table 41 Network entries

Field	Description
Network IP Address	IP address for the protected network.
Network Mask	Subnet mask for the protected network. Non-contiguous masks are valid on ETEP PEPs version 1.4 and later.



TIP

You can use a network mask of 255.255.255.255 to specify an individual address, or host. For example, you might want to do this for traffic from devices such as a Lotus Notes server that needs to be sent in the

clear.

ETPM accepts non-contiguous network masks, which allow you to create policies between particular addresses in your network. For example, a network of 10.0.0.1 with a mask of 255.0.0.255 allows all devices with an IP address of 10.x.x.1 to be managed by a particular policy. This feature is available only with ETEP PEPs. See [“Using Non-contiguous Network Masks” on page 162](#) for more information.

Advanced Uses for Networks in Policies

If you are familiar with network addressing and network masks, you can use subnetting to make your policies more efficient.

- [“Grouping Networks into Supernet” on page 161](#)
Use supernetting to reduce the number of SAs and keys on each PEP in large deployments.
- [“Using Non-contiguous Network Masks” on page 162](#)
Use non-contiguous network masks to apply policies to a specific IP address scheme.

Grouping Networks into Supernets

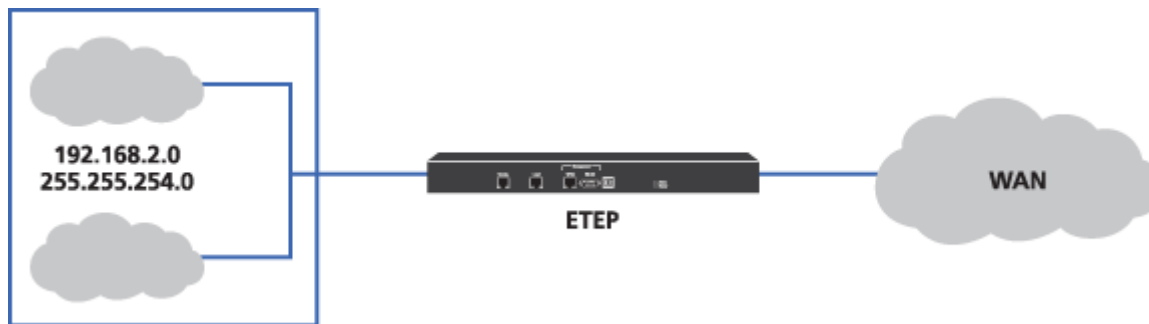
Working with large networks, a considerable number of security associations (SAs) and keys can result on each PEP. One way to avoid this is to look for subnetworks within each network set that have contiguous addressing. You can combine these subnets to reduce the number of SAs and keys on each PEP.

In [Figure 55](#), if you set up each of these networks as a separate network in ETPM, and the policy encrypts traffic between these two networks and five other networks, the PEP for this network set would contain 10 SAs and keys for each direction.

Figure 55 Two networks with contiguous addressing



As illustrated in [Figure 56](#), the two networks 192.168.2.0 with subnet mask 255.255.255.0 and 192.168.3.0 with subnet mask 255.255.255.0 could be grouped into one network 192.168.2.0 with subnet mask 255.255.254.0.

Figure 56 Two networks with contiguous addressing defined as a supernet

If you group the two networks into a supernet and the policy encrypts traffic between these two networks and five other networks, the PEP for this network set would contain only five SAs and keys for each direction, instead of 10.

 **NOTE**

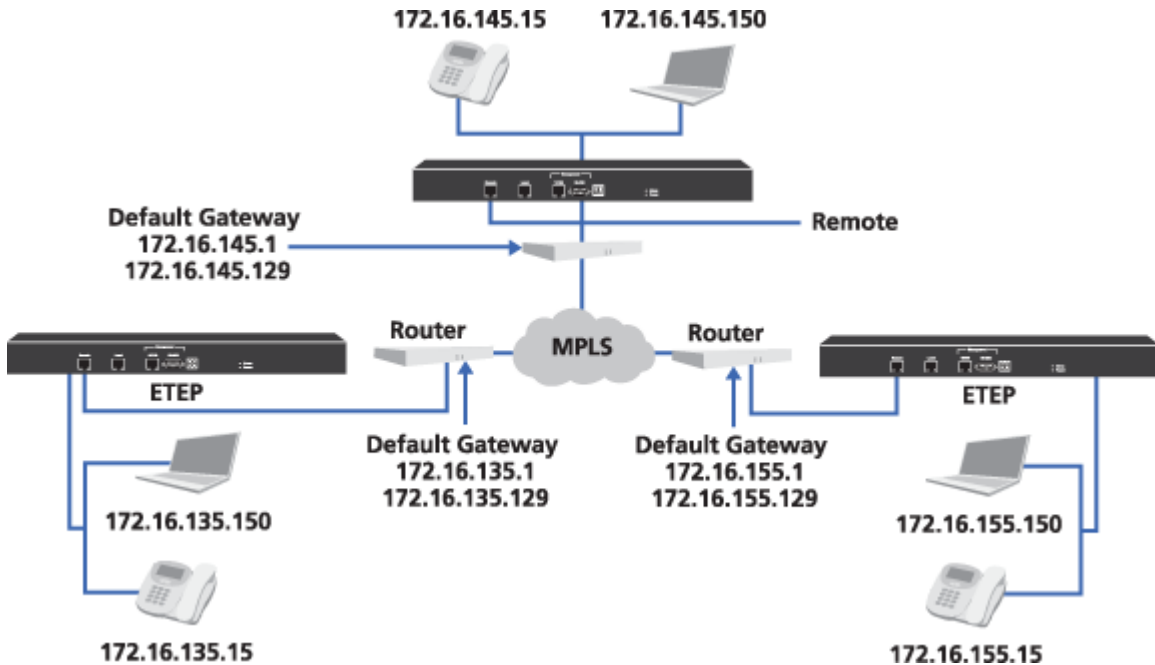
Where the subnetwork addresses are not completely contiguous, grouping these networks can result in the inclusion of an unintended subnetwork.

Using Non-contiguous Network Masks

Non-contiguous masks are useful when you want to create a policy for devices in a network that contain a specific octet within an IP address. Non-contiguous network masks are available on ETEP PEPs version 1.4 and later.

The following example demonstrates the use of non-contiguous network masks to pass unencrypted traffic from specific addresses while encrypting everything else. [Figure 57](#) depicts a mesh network in which all traffic on each subnet is encrypted. A router is located on each of the PEP's remote ports, which means that all traffic to it is encrypted. However, the router port that is connected to the PEP's remote port is the default gateway for the site. In order to manage the router, traffic from the laptop needs to pass in the clear. VoIP traffic also needs to pass in the clear. Each site uses IP addresses of x.x.x.129 and x.x.x.1 for the default gateway.

Figure 57 Networks with non-contiguous network masks are used in a bypass policy that encompasses all the x.x.x.1 and x.x.x.129 addresses



Defining networks with non-contiguous masks allows you to create a single bypass policy that encompasses all the .1 and .129 addresses, enabling the local sites on the 172.16.x.x network to manage the devices on the remote port side of the PEP. By defining the networks as shown in [Table 42](#), you eliminate the need to create individual bypass policies for each subnet in the network.

Table 42 Networks definitions

IP Address	Network Mask
0.0.0.129 (laptops)	0.0.0.255
0.0.0.1 (VoIP phones)	0.0.0.255
172.16.0.0 (any traffic on this network)	255.255.0.0

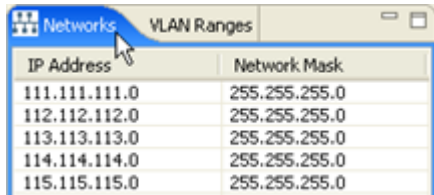
 **NOTE**

When you use non-contiguous network masks, the network set must include a PEP that supports the feature (ETEP v.1.4 and later). In addition, all network sets in a policy must include supporting PEPs. ETPM prevents you from dragging non-supporting elements into a network set or policy when non-contiguous networks masks are in use.

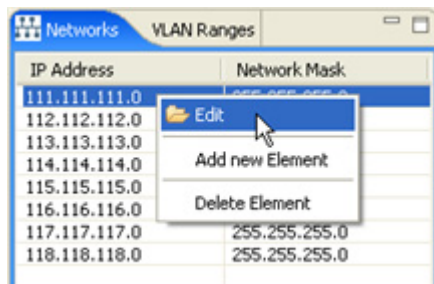
Editing Networks

To edit an existing network:

- 1 In the EncrypTight Components view, click the **Networks** tab.



- 2 Right-click the desired network, click **Edit**.



- 3 Change the entries of the desired fields in the editor.
[Table 41 on page 160](#) describes the entries on the network editor.
- 4 Click **Save** when all entries are modified as desired.

Deleting Networks

Occasionally, you might want to delete a network. For example, if the structure of a network changes, the network you set up in ETPM might not be needed.

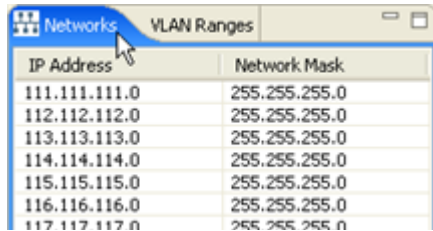


CAUTION

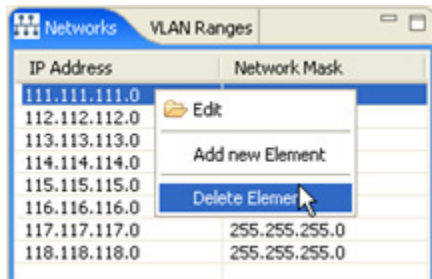
*Do not delete any Networks currently used by any network sets. Prior to deleting a network, modify any network sets using that network to use another network. If you delete a network that is currently used in a policy or a network set, you can create configuration errors that might prevent you from deploying your policies. In this case, check the Policy view to find the components with configuration errors. Correct the errors and then click **Deploy**.*

To delete a network:

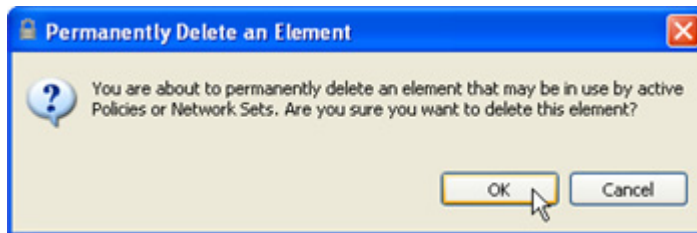
- 1 In the EncryptTight Components view, click the **Networks** tab.



- 2 Right-click the desired Network and click **Delete**.



- 3 Click **OK** on the Permanently Delete an Element Window.



13 Managing Network Sets

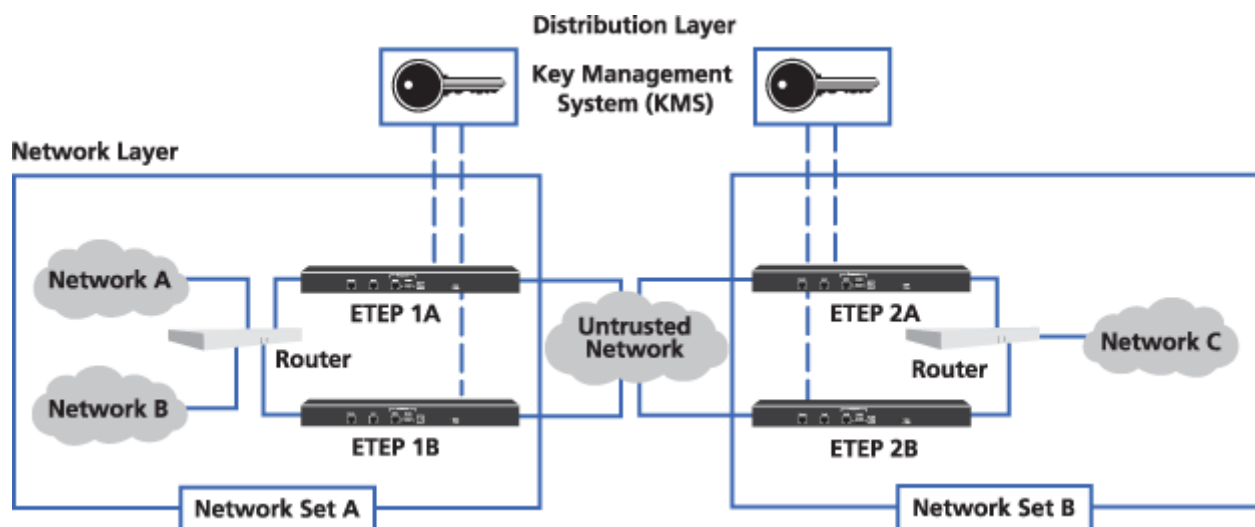
A network set is a collection of IP networks, the associated PEPs, and a default ETKMS. A network set is treated as a single entity in a policy.

This section includes the following topics:

- Types of Network Sets
- Adding a Network Set
- Importing Networks and Network Sets
- Editing a Network Set
- Deleting a Network Set

Figure 58 shows two network sets. Network Set A contains two networks protected by two PEPs and Network Set B contains one network protected by two PEPs. Network Set A uses ETKMS 1 as its default Key Management System and Network Set B uses ETKMS 2 as its default Key Management System. The default Key Management System distributes the keys and policies to the PEPs within a network set.

Figure 58 Network Sets



Types of Network Sets

The following examples illustrate the different types of network sets:

- Subnet
- Load balanced network
- Collection of networks
- A network set that does not contain any PEPs

Figure 59 Network set for a subnet

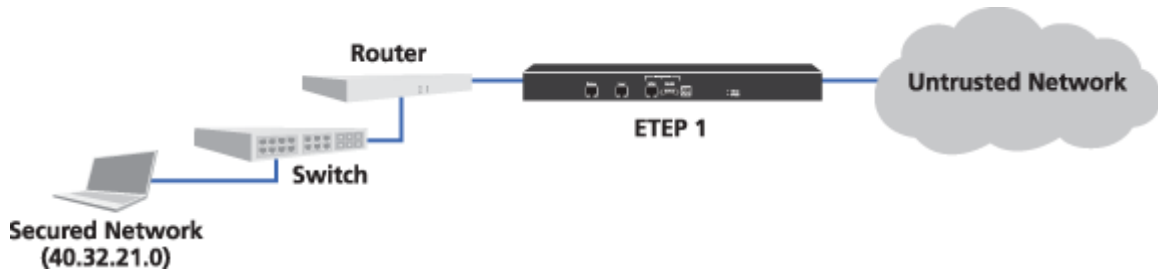


Figure 59 illustrates a network set consisting of a single network and a single PEP. In ETPM, this network set would include PEP 1 and the network IP address and mask:

IP address	Mask
40.32.21.0	255.255.255.0

Figure 60 Network set for a load balanced or redundant network

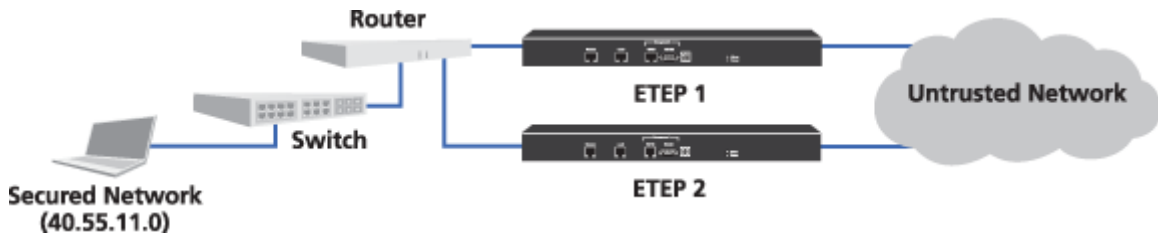


Figure 60 illustrates a load balanced or redundant network with multiple access to a single network with two PEPs. In ETPM, this network set includes both PEP 1 and PEP 2, and the network IP address and mask:

IP address	Mask
40.55.11.0	255.255.255.0

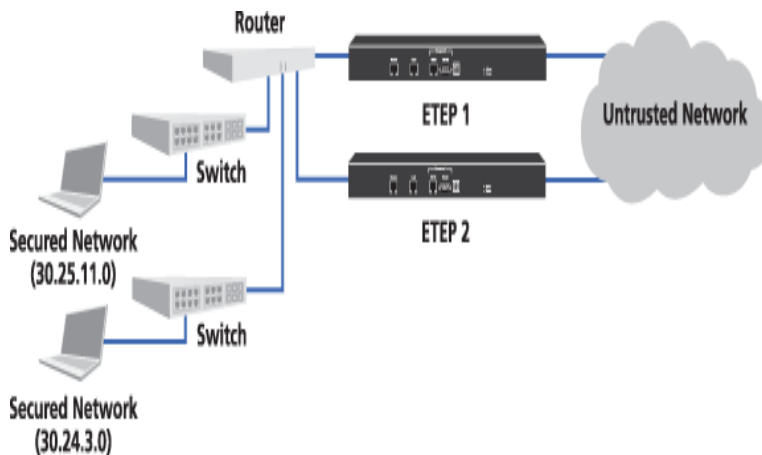
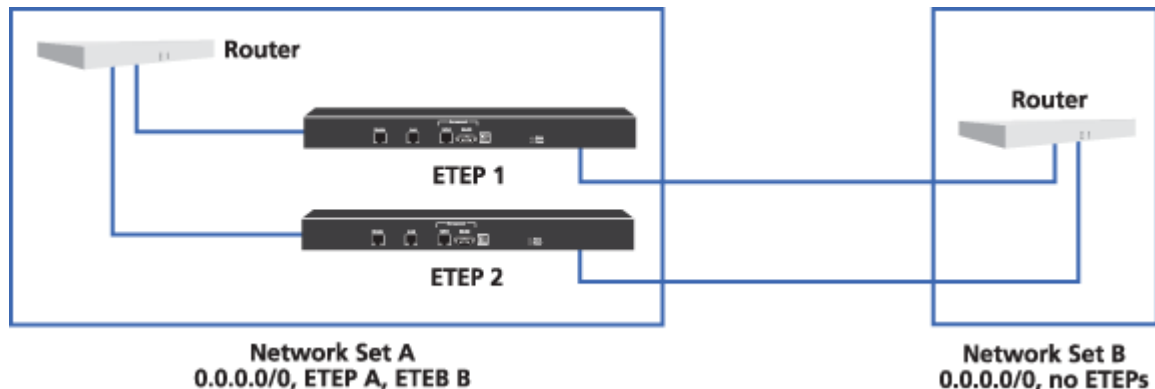
Figure 61 Network set for a collection of networks

Figure 61 illustrates a network set comprised of two networks and two PEPs. In ETPM, this network set includes both PEP 1 and PEP 2, and both network IP addresses and masks.

IP address	Mask
30.25.11.0	255.255.255.0
30.24.3.0	255.255.255.0

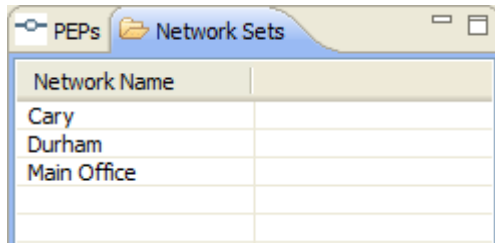
Figure 62 Network set that does not include a PEP

A network set does not have to include any PEPs. This is useful if you have PEPs that are encrypting traffic between two routers that need to exchange routing protocols. If the PEPs are encrypting all traffic, the routers cannot see the information in the routing packets. To allow the routers to exchange routing information create a clear policy for the routing protocol, for example OSPF (protocol 89). Create one network set with a wildcarded network (0.0.0.0) that includes PEP 1 and PEP 2. Create a second network set with a wildcarded network (0.0.0.0), but without any PEPs. Then using these two network sets, you can create a point-to-point policy that passes protocol 89 packets in the clear.

Adding a Network Set

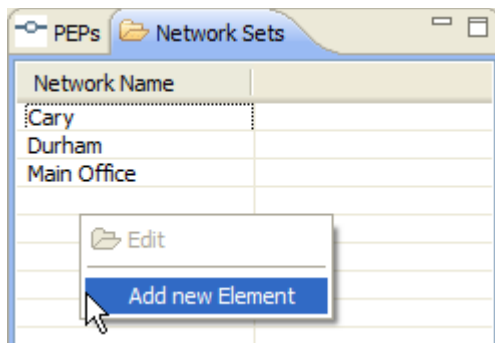
To add a Network Set:

- 1 In the EncryptTight Components view, click the **Network Sets** tab.



The Network Sets view lists the network sets added previously. You can sort the list of network sets by clicking the **Network Name** column header.

- 2 Right-click anywhere in the Network Set view and click **Add new Element**.



- 3 Create the network set in the Network Set editor as described in [Table 43](#). The Network Set editor is shown in [Figure 63](#).
- 4 Click **Save** when complete.

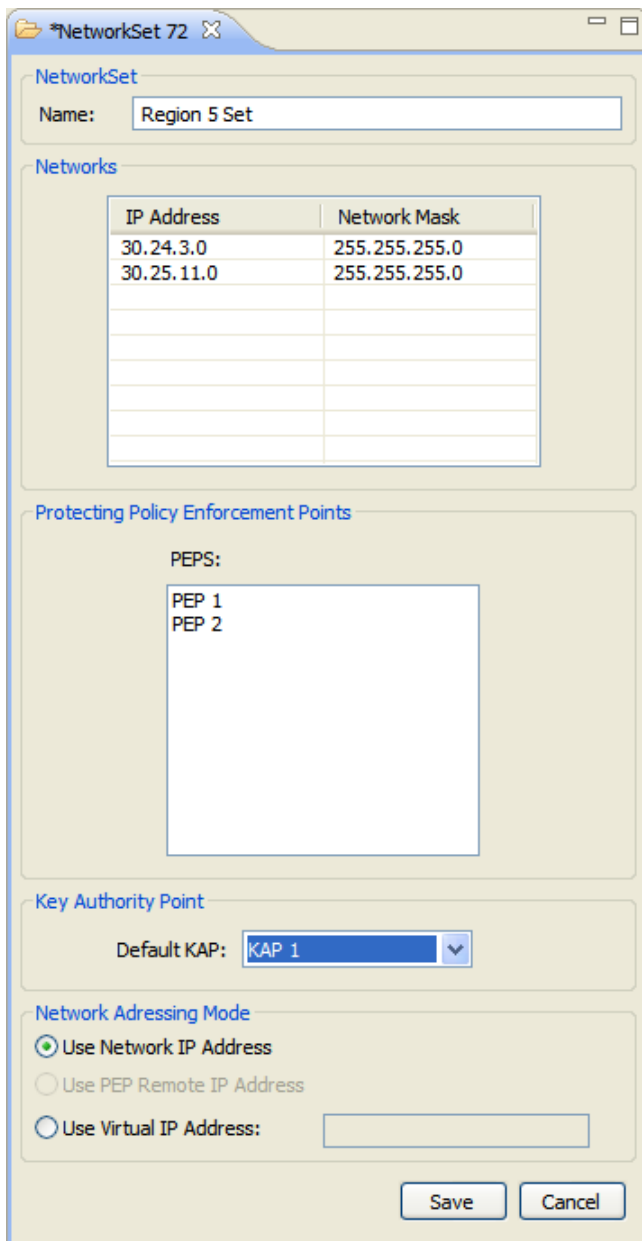
Table 43 Network Set fields

Field	Description
Name	Enter a unique name to identify the network set. Names can be 1 - 40 characters in length. Alphanumeric characters and spaces are valid. The special characters <, >, &, “*”, ?, /, \, : and cannot be used in the network set name. Names are not case sensitive.
Networks	Click the Networks tab in the EncryptTight Components view and drag the appropriate networks to the Networks list on the Network Set editor. A network set can consist of up to 9 networks. <ul style="list-style-type: none"> • You can also edit a network from this editor. Right-click the desired network and click Edit. • To remove a network from this list, right-click the desired network and click Remove Element. The network is removed only from this network set.
Protecting Policy Enforcement Points	Click the PEPs tab in the EncryptTight Components view and drag the appropriate PEPs to the PEPs list on the Network Set editor. To remove a PEP from this list, right-click the desired PEP and click Remove Element . The PEP is removed only from this network set.

Table 43 Network Set fields (continued)

Field	Description
Key Management System	Select the desired Key Management System from the Default ETKMS list. You must select a ETKMS even if the network set does not include a PEP. If you create a policy that includes a network set that does not have a ETKMS, you will not be able to deploy that policy.
Network Addressing Mode	<p>Select the desired network addressing mode. The network addressing mode specifies the source IP address used in the packet header.</p> <ul style="list-style-type: none"> • Use Network IP Address (default) - original packet header containing the network's IP address is used for all outgoing packets. • Use PEP's Remote IP Address - the PEP's remote port IP address is inserted into the packet header for all outgoing packets. This option is not available if the network set contains more than one PEP. • Use Virtual IP Address - the virtual IP address is inserted into the packet header for all outgoing packets. If you select this option, enter the IP address to use as the source address for outgoing packets in the Virtual IP Address box. <p>Depending on the type of PEP selected and its configuration, some options may not be available. ETEP PEPs preserve the original network address by default and must be explicitly configured to use any other mode. For more information on how to configure your PEP, see the configuration chapter for your PEP.</p> <p>For more information on network addressing modes, see "Network Addressing for IP Networks" on page 35.</p> <p>This setting can be overridden by settings in a policy. For more information, see "Addressing Mode" on page 185.</p>

Figure 63 Network Set editor



Importing Networks and Network Sets

If you need to work with a large number of networks and network sets, you can save time by importing the data into ETPM. You can create a CSV file that lists the networks and network sets that you need and import the file. The default ETKMS and the PEPs used in the network sets must have been added to ETEMS previously or the import will fail.

To create the import file, enter the data in a spreadsheet (such as Excel) and save it as a .csv file, or enter the data directly in a text editor such as Notepad. You must adhere to the formats shown in [Figure 64](#) and [Figure 65](#). The first line in the file must be Version1.0, while the pound symbol (#) indicates a comment

line and is ignored by ETPM during the import operation. In the CSV file, commas are used to delineate one field or item from the next.

The format of the CSV file is as follows:

```
Version1.0
network,<networkid>,<ip address>,<mask>
networkSet,<name>,<etkmsName>,networkIds,<list of network IDs>,peps,<list of PEP names>
```

Figure 64 Networks and network sets import document format in Excel

	A	B	C	D	E	F	G	H
1	Version1.0							
2	#Networks							
3	#Format as: network	<networkId>	<ip address>	<mask>				
4	network	Raleigh 2	192.168.3.44	255.255.255.0				
5	network	Cary	192.168.5.44	255.255.255.0				
6	network	Durham	192.168.88.10	255.255.255.0				
7	network	Raleigh North	192.168.3.98	255.255.255.0				
8	network	Morrisville	192.168.122.22	255.255.255.0				
9	#							
10	#NetworkSets							
11	#Format as: networkSet	<name>	<etkmsName>	networkIds	<list of network ids>		peps	<list of pep names>
12	networkSet	Main Office	ETKMS Main	networkIds	Raleigh 2	Raleigh North	peps	Main PEP 1
13	networkSet	Cary	ETKMS Branch 1	networkIds	Cary	Morrisville	peps	Branch 1 PEP
14	networkSet	Durham	ETKMS Branch 1	networkIds	Durham		peps	Branch 2 West PEP

Figure 65 Networks and network sets import document format in a text editor

```
Version1.0
#Networks
#Format as: network,<networkId>,<ip address>,<mask>
network,Raleigh 2,192.168.3.44,255.255.255.0
network,Cary,192.168.5.44,255.255.255.0
network,Durham,192.168.88.10,255.255.255.0
network,Raleigh North,192.168.3.98,255.255.255.0
network,Morrisville,192.168.122.22,255.255.255.0
#
#NetworkSets
#Format as: networkSet,<name>,<etkmsName>,networkIds,<list of network ids>,,peps,<list of pep names>
networkSet,Main Office,ETKMS Main,networkIds,Raleigh 2,Raleigh North,peps,Main PEP 1
networkSet,Cary,ETKMS Branch 1,networkIds,Cary,Morrisville,peps,Branch 1 PEP
networkSet,Durham,ETKMS Branch 1,networkIds,Durham,,peps,Branch 2 West PEP
```

Table 44 Networks and network sets import format description

Attribute	Description
network	Keyword that indicates a network definition follows.
networkId	Name that uniquely identifies the network.
ip address	IP address of the network.
mask	Subnet mask for the network.
networkSet	Keyword that indicates a network set definition follows.
name	Name that uniquely identifies the network set.
etkmsName	Name of the default ETKMS for the network set. This must be a ETKMS that has already been added in ETEMS.
networkIds	Keyword that indicates a list of one or more network identifiers follows.
list of network IDs	In the CSV file, each identifier must be separated by a comma. In a spreadsheet, place each identifier in a cell by itself. Each identifier must have been defined previously in the file.

Table 44 Networks and network sets import format description

Attribute	Description
peps	Keyword that indicates a list of one or more PEP names follows.
list of PEP names	In the CSV file, each PEP name must be separated by a comma. In a spreadsheet, place each PEP name in a cell by itself. Each PEP must have been added to ETEMS previously.

To import networks and network sets into ETPM:

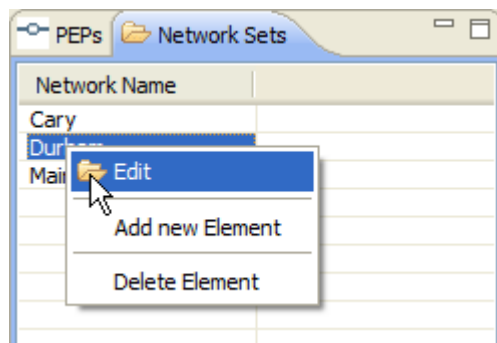
- 1 Create a CSV file that identifies the networks and network sets.
- 2 In ETPM, choose **File > Import Networks**, select the CSV file and click **OK**.

If ETPM detects an error in the CSV file, none of the networks or network sets are imported. ETPM displays an error message that includes the number of the line in the file that contains the error along with a brief description of the problem. The message also indicates the column number with the error, which is useful if you created the CSV file in a spreadsheet (the column number does not apply to the CSV file in a text editor).

Editing a Network Set

To edit a Network Set:

- 1 In the EncrypTight Components view, click the **Network Set** tab.
- 2 Right-click the desired network set and click **Edit**.



- 3 Change the entries of the desired fields in the editor.
[Table 43 on page 170](#) describes the entries on the network set editor.
- 4 Click **Save** when all entries are modified as desired.

Deleting a Network Set

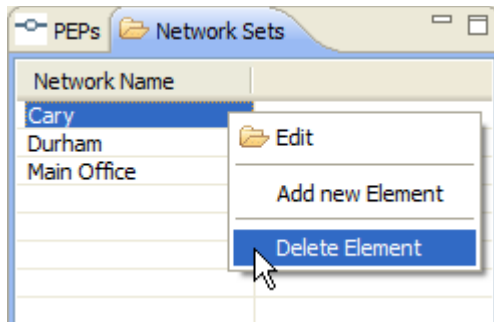
You might need to delete a network set if the structure of a network changes or if the network set is empty because the networks were removed.

 **CAUTION**

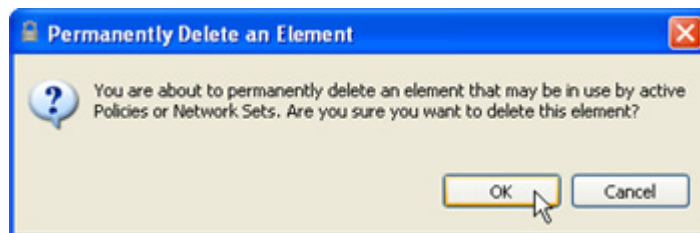
Prior to deleting a network set, modify any policies using that network set to use another network set. If you delete a network set that is currently used in a policy, you can create configuration errors that might prevent you from deploying your policies. In this case, check the Policy view to find the components with configuration errors. Correct the errors and then click **Deploy**.

To delete an existing network set:

- 1 In the EncryptTight Components view, click the **Network Set** tab.
- 2 Right-click the desired network set and click **Delete Element**.



- 3 Click **OK** on the Permanently Delete an Element Window.



14 Creating VLAN ID Ranges for Layer 2 Networks

If the network uses VLAN ID tags, you have the option of creating policies that select traffic with specific VLAN ID tags or within a range of VLAN ID tags. If you do not include VLAN ID tags in a new Layer 2 policy, the policy is applied to all network traffic.

VLAN ID tags are used to create logical networks within a larger physical network. This is often used to separate network traffic by departments, such as Finance or Human Resources. By creating policies that act on specific VLAN ID tags or a range of VLAN ID tags, you can encrypt, pass in the clear, or drop traffic at the logical level (in this case by department). Traffic that does not match the VLAN ID tag (or range of tags) specified in the policy is dropped.

ETEP PEPs accept only single VLAN ID tags in policies.

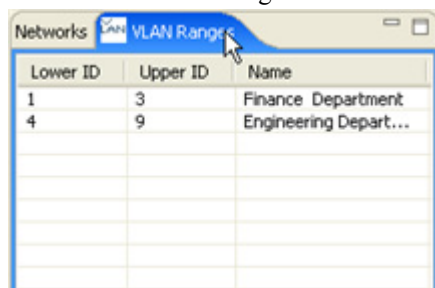
This section includes the following topics:

- [Adding a VLAN ID Range](#)
- [Editing a VLAN ID Range](#)
- [Deleting a VLAN ID Range](#)

Adding a VLAN ID Range

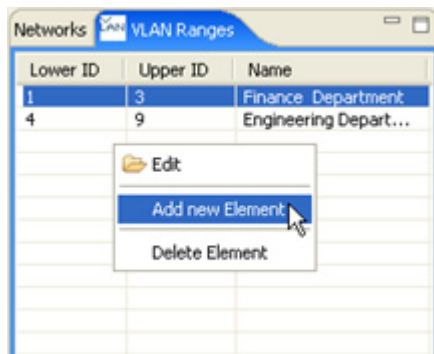
To add a new VLAN ID Range:

- 1 From the EncryptTight Components view, click the **VLAN Ranges** tab. The VLAN Ranges tab lists all of the VLAN ID ranges.



Lower ID	Upper ID	Name
1	3	Finance Department
4	9	Engineering Depart...

- 2 Right-click anywhere in the VLAN Ranges view and then click **Add new Element**.



- 3 Create the VLAN range in the editor as described in [Table 45](#).
- 4 Click **Save** when complete.

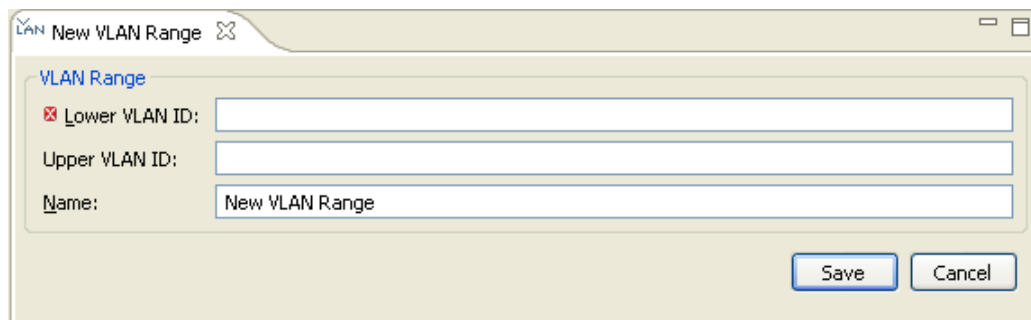
NOTE

VLAN ranges are not supported on ETEP PEPs. If you enter a range, the ETEP uses only the lower VLAN ID. We recommend entering the same value for the upper and lower VLAN ID when working with ETEP PEPs.

Table 45 VLAN ID range entries

Field	Description
Lower VLAN ID	Enter the lower range limit in the range 1 to 4094.
Upper VLAN ID	Enter the upper range limit in the range 1 to 4094.
Name	Enter a unique name to identify this particular VLAN Range. Names can be 1 - 40 characters in length. Alphanumeric characters and spaces are valid. The special characters <, >, &, ", *, ?, /, \, : and cannot be used. Names are not case sensitive.

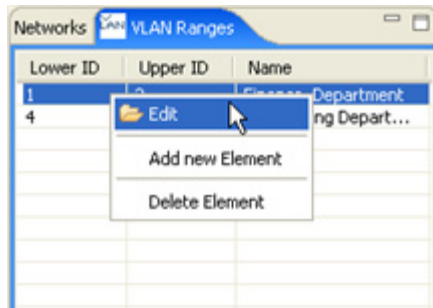
Figure 66 VLAN range editor



Editing a VLAN ID Range

To edit a VLAN ID range:

- 1 In the EncryptTight Components view, click the **VLAN Ranges** tab.
- 2 Right-click the desired VLAN ID range and click **Edit**.



- 3 Change the entries of the desired fields in the editor.
[Table 45 on page 178](#) describes the entries on the VLAN Range editor.
- 4 Click **Save** when all entries are modified as desired.

Deleting a VLAN ID Range

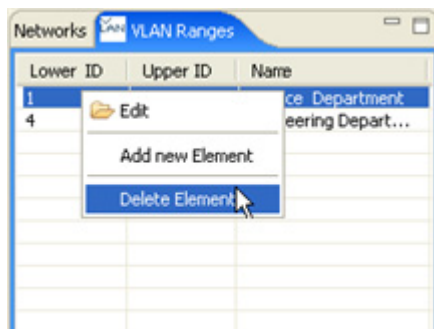
If changes are made to a network or VLAN, you might need to delete VLAN ID ranges.

CAUTION

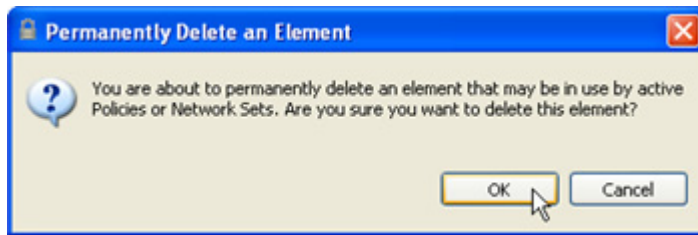
Deleting a VLAN ID or range that is currently used in a policy can cause unexpected results. You will still be able to deploy policies, but traffic with the ID or within the range can get encrypted, passed in the clear, or dropped by mistake.

To delete an existing VLAN ID range:

- 1 In the EncryptTight Components view, click the **VLAN Ranges** tab.
- 2 Right-click the desired VLAN ID range and click **Delete Element**.



- 3 Click **OK**.



15 Creating Distributed Key Policies

From the Policy view, you can add, modify, and delete policies for Layer 3/Layer 4 IP networks and Layer 2 Ethernet networks.

This section includes the following topics:

- [Policy Concepts](#)
- [Adding Layer 2 Ethernet Policies](#)
- [Adding Layer 3 IP Policies](#)
- [Adding Layer 4 Policies](#)
- [Policy Deployment](#)
- [Editing a Policy](#)
- [Deleting Policies](#)

Policy Concepts

A policy specifies what traffic to act on and what action to take. Each PEP can store a large number of policies. As network traffic arrives, each packet or frame is examined by the PEP, and processed based on selection criteria such as IP addresses, ports, protocols, or VLAN tags. When the PEP receives a packet or frame that meets the criteria used in one of its policies, it takes one of three actions: it encrypts the packet or frame, bypasses it (passes in the clear), or drops it.

In addition to selection criteria and actions, each policy specifies:

- What priority a policy has in relation to other policies
- How often keys are renewed and policy lifetimes are refreshed
- What encryption and authentication methods to use
- Whether key generation is handled by a single ETKMS or the default ETKMSs in each network set
- Which addressing mode the PEPs in the policy should use
- Whether to reduce the policy size for an IP policy

Related topics:

- [“Policy Priority” on page 182](#)
- [“Schedule for Renewing Keys and Refreshing Policy Lifetime” on page 182](#)
- [“Policy Types and Encryption Methods” on page 183](#)

- “Key Generation and ETKMSs” on page 185
- “Addressing Mode” on page 185
- “Using Encrypt All Policies with Exceptions” on page 185
- “Policy Size and ETEP Operational Limits” on page 186
- “Minimizing Policy Size” on page 187

Policy Priority

You can assign a priority from 1 to 65000 to each policy that you create. The policy priority specifies the order in which policies are processed on the PEP. For each incoming packet or frame the PEP searches through the list of policies, starting with the policy that has the highest priority, until it finds a match. When it finds a match, the PEP processes the packet or frame according to the settings in the policy. As you create policies, carefully consider the policy priority that you choose.

If your policies are not being implemented as expected, check the priorities assigned to the policies. Incorrect prioritization can produce unexpected results. For example, policy A is a clear policy for a specific destination network for any protocol and has the highest priority. Policy B is an encrypt policy for the same destination network with a particular protocol, but it has a lower priority. Because policy A has the higher priority, all traffic passes and none of the traffic is encrypted.

Schedule for Renewing Keys and Refreshing Policy Lifetime

The Renew keys/Refresh lifetime value specifies the length of time that the keys and policies will be active. According to the schedule specified in the policy, the ETKMS sends new keys to the PEPs. The previous keys are maintained on the PEP for up to five minutes to ensure that no traffic interruption occurs. For Bypass and Drop policies (which do not have keys), the policy lifetimes are refreshed.

You schedule the key renewal and policy refresh in an interval of hours or set a daily renewal at a specified time.

- **Hours** - enter the re-key interval in hours between 0 and 65535 hours. Use 0 to effectively specify that the keys and policies never expire and never update. (Technically, when you enter 0, ETPM inserts the value of 61320 hours, or 7 years.) Most likely, you will only use 0 hours for drop and clear policy types.
- **Daily** - enter the re-key time using the 24 hour system clock set to the required local time of the ETPM workstation. The re-key time will translate to the local times of the ETKMSs and PEPs that might be located in other time zones.



TIP

Management traffic increases during the policy rekey and renew lifetime process. This is true for both manual and automatic rekeys. If you schedule all policies to rekey at the same time, the ETKMSs will send new keys to all of their PEPs at the same time, causing an increase in traffic throughout your network. You can reduce the traffic and processing time by staggering the rekey schedule specified for each policy. For example, one policy could be set to rekey at 1:00 AM while another policy could be set to rekey at 1:30 AM. This significantly reduces the management traffic and PEP processing time.

**TIP**

Network connectivity problems can prevent new keys from being distributed to the PEPs before the old keys expire. If you experience problems of this nature, see [“Solving Network Connectivity Problems” on page 248](#) for suggested workarounds to prevent interruptions.

Policy Types and Encryption Methods

The type of policy specifies the action applied to packets that match the protocol and networks included in this policy. You can choose from the following types:

- **Drop** - drops all packets matching this policy.
- **Bypass** - passes all packets matching this policy in the clear.
- **IPSec** - encrypts or decrypts all packets matching this policy. (For Layer 2 Ethernet policies, this option is **Encrypt**.)

The following topics describe how traffic is protected in an encryption policy:

- [“Encapsulation” on page 183](#)
- [“Encryption and Authentication Algorithms” on page 184](#)

Encapsulation

To provide encryption and authentication, the PEPs use the EncrypTight Encapsulating Security Payload protocol (CE-ESP). CE-ESP is Black Box’s packet encapsulation protocol that is based on the IPSec ESP protocol standards.

Layer 2: Ethernet payload encryption

In Layer 2 policies, the CE-ESP protocol preserves the original Ethernet header information and encrypts only the Ethernet payload, as shown in [Figure 67](#).

Figure 67 Ethernet frame encryption



Layer 3: IPSec Tunnel mode with original IP header preservation

In Layer 3 IP policies, a copy of the original IP header is used as the outer header and the original header and payload are encrypted, as shown in [Figure 68](#).

Figure 68 IP packet encryption



Layer 4: IPSec Transport mode for Layer 4 payload encryption

EPEP PEPs have an option to encrypt only the Layer 4 payload. The TCP and UDP header information remains in the clear, as shown in [Figure 69](#). All other Layer 4 headers are encrypted.

Figure 69 Data payload encryption

Encryption and Authentication Algorithms

For Layer 3 IP policies, you can specify the encryption and authentication algorithms that you want to use. The encryption algorithms include the Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES).

AES is a symmetric block cipher capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. Triple DES, or 3DES, is a more secure variant of DES. 3DES uses a key length of 168 bits. The Data Encryption Standard (DES) is a symmetric block cipher with a block size of 64 bits and a key length of 56 bits.

The authentication algorithms available include Secure Hash Algorithm 1 (HMAC-SHA-1) and Message Digest #5 (HMAC-MD5). Both are hash algorithms. HMAC-SHA-1 is more secure than HMAC-MD5.

Layer 2 Ethernet encryption policies utilize AES with 256-bit keys to encrypt and decrypt the data and HMAC-SHA-1 to provide data origin authentication and data integrity.

Layer 4 IP encryption policies use AES-256 for encryption and HMAC-SHA-1 for authentication. The ETEP PEPs do not support 3DES or HMAC-MD5 at Layer 4.

ARIA Encryption

In addition to the standard encryption algorithms listed above, the ARIA encryption algorithm is available on ETEP PEPs. ARIA provides 256-bit encryption, and is implemented in software.

Note the following usage guidelines and constraints:

- ARIA-256 is available for use in Layer 3 and Layer 4 policies. Layer 2 Ethernet encryption policies do not support ARIA.
- ARIA-256 is incompatible with the ETEP's FIPS mode of operation. Disable FIPS mode on the ETEP prior to using ARIA in encryption policies.
- ARIA-256 is available only when using the local ETKMS software. External ETKMSs do not support policies that use ARIA encryption.

To use ARIA in an encryption policy, do the following:

- 1 Quit EncrypTight if it is running (**File > Exit**).
- 2 Edit the EncrypTight `config.ini` file. The file is located in the `<installDir>\configuration` directory, where `<installDir>` is the directory in which EncrypTight is installed.
 - a Using a text editor such as Notepad, open the `config.ini` file.
 - b Change the `AriaSupport` setting from `false` to `true`. The modified line should look like this:


```
AriaSupport=true
```
 - c Save the file, and then close the text editor.
- 3 Restart EncrypTight.
- 4 In ETPM, select ARIA as the encryption algorithm in the policy editor. This algorithm is available in any Layer 3 or Layer 4 policy type: mesh, point-to-point, multicast, or hub and spoke. After defining the encryption policy, deploy the policy to the ETEPs.

Key Generation and ETKMSs

With multicast IP policies and Layer 2 Ethernet policies, you choose a single ETKMS to generate and distribute the keys. With point-to-point, hub and spoke, and mesh IP policies there are two options for specifying which ETKMSs generate and distribute keys.

- **By Network Set** - The default ETKMS within each network set generates and distributes the keys to the PEPs included in those network sets.
- **Global ETKMS** - A single ETKMS, referred to as a global ETKMS, generates the keys and sends them to the default ETKMSs in each network set for distribution to all of PEPs included in the policy.

Addressing Mode

When you create network sets in the network sets editor, you specify the IP address the PEPs will use in the outer header of the encrypted packets. The options include the original IP address of the packets received at the PEP's local port (the default setting), the remote port IP address of the PEP, or a virtual IP address that is configured as part of a network set. The second two options are used when the original source IP address must be concealed or when traffic must be routed over the internet.

Even when you configure network sets to conceal the original source IP addresses, you might need to preserve the original IP addresses for other traffic that is routed through the same network sets. For example, you might need to transmit traffic that must comply with Service Level Agreements.

To handle these situations, you can create additional policies that use the same network sets, but override the specified network addressing mode. In the policy editor, the network addressing mode can use one of two options:

- Preserve only the original internal network addresses. The source and destination addresses in the IP header are sent in the clear. The protocol and port, as well as the payload of the packet are encrypted. This is referred to as a Layer 3 policy.
- Preserve the original internal network address, protocol, and port. The source and destination addresses, protocol, and port in the IP header are sent in the clear. With this option, only the payload of the packet is encrypted. This allows you to send the Layer 4 header information in the clear for traffic engineering and Service Level Agreement management (for example, Quality of Service controls or NetFlow statistics monitoring). This is referred to as a Layer 4 policy.

Related topics:

- [“Network Addressing for IP Networks” on page 35](#)
- [“Adding a Network Set” on page 170](#)
- [“Encapsulation” on page 183](#)

Using Encrypt All Policies with Exceptions

You can design your policies many different ways for the same results. If you design your policies based on chunks of data such as which port or which source or destination address encrypts, drops, or passes in the clear, a large number of policies can result. With a large number of policies, the policy management overhead increases and keeping track of the priority of each policy can become difficult. You can simplify this process by doing the following:

- 1 Create a policy to encrypt all data to and from all networks. Assign this policy a relatively low priority to ensure that any missed data will at least pass encrypted.
- 2 Design a pass in the clear policy and a drop policy with a higher priorities.

Table 46 illustrates policies for a mesh network that will pass Protocol 17 (UDP) traffic in the clear, drop all protocol 55 (IP mobile) traffic, and encrypt all other traffic.

Table 46 Encrypt all policy with exceptions

Policy	Policy Type	Priority	Action	Protocol Covered
1	Mesh	100	Encrypt	All
2	Mesh	200	Drop	55
3	Mesh	300	Pass in Clear	17

In this case, we started with the assumption that our main job was to encrypt traffic and then decide which traffic to drop or pass in the clear. The PEP analyzes each packet starting with the highest priority policy.

The alternative is to decide which traffic should be encrypted, which traffic should be passed in the clear, and which traffic should be dropped. With this approach, you risk creating more policies to manage than you need and increasing the management traffic on the network. You could also easily miss encrypting important traffic.

Policy Size and ETEP Operational Limits

Various combinations of factors can reach or exceed the operational limits of the ETEP PEP, including memory, processor speed, and the size of the policy file. Another core issue is the number of security associations (SAs) a PEP can support.

An SA identifies what traffic to act on, what kind of security to apply, and the device with which the traffic is being exchanged. SAs typically exist in pairs, one for each direction (inbound and outbound). The policies deployed from ETPM create SAs between the PEPs. A simple point-to-point policy creates two SAs on each PEP. More complex configurations such as a mesh policy create more SAs.

The policy file is an XML file sent to each PEP that identifies the type of policy, the ETKMSs used, the policy lifetime, and the kind of traffic the policy affects. It also identifies the networks to be protected and the PEPs to be used.

The size of a policy file is determined by the type of policy, the number of PEPs, and the number of networks protected. On the ET0010A, the maximum size for the policy file is 512 KB. For the ET0100A, the maximum size is 1024 KB.

If the policy file is larger than the maximum size, the rekey processing time on the PEP can exceed the system timeout parameters. For example, with the ET0010A the rekey processing time for a 512 KB policy file is approximately three minutes. If the rekey processing takes longer than this, timeouts and errors occur that severely affect overall system performance. When timeouts and errors occur, keys can expire or a policy might not actually be deployed.

To prevent this from happening, ETEP PEPs generate error messages and reject policy files that are larger than the maximum size. The error messages are recorded in the ETKMS log file. For information about viewing the ETKMS log file, see [“ETKMS Log Files” on page 241](#).

Minimizing Policy Size

Using EncrypTight with large, complex networks with multiple subnets protected by separate PEPs can result in a large number of SAs on each PEP. The increased management traffic for renewing keys and refreshing policy lifetimes could adversely affect the performance of EncrypTight. If you do not require policy filtering based on subnets located with each PEP, use the minimize policy size feature to avoid this. This feature is not applicable to Layer 2 Ethernet policies.

The Minimize Policy Size feature includes two options, depending on the type of policy. You can select **Ignore source IP address** for any IP policy. For mesh policies, you can select either **Ignore source IP address** or **Apply to all traffic**.

When you enable the Ignore source IP address option:

- The source network address for *outbound* traffic is replaced with an all networks wildcard address (0.0.0.0/0)
- The destination network address for *inbound* traffic is replaced with an all networks wildcard address (0.0.0.0/0)

This results in a significant reduction in policy size and keys in each PEP associated with the policy.

The Apply to all traffic option is useful for large mesh networks when you know that each PEP only sends traffic to other PEPs using the same policy. Selecting this option applies the policy to all traffic, inbound and outbound, regardless of the source and destination addresses or ports. If the policy specifies encryption, all PEPs associated with the policy use the same key set, reducing the number of policy entries and SAs on each PEP.

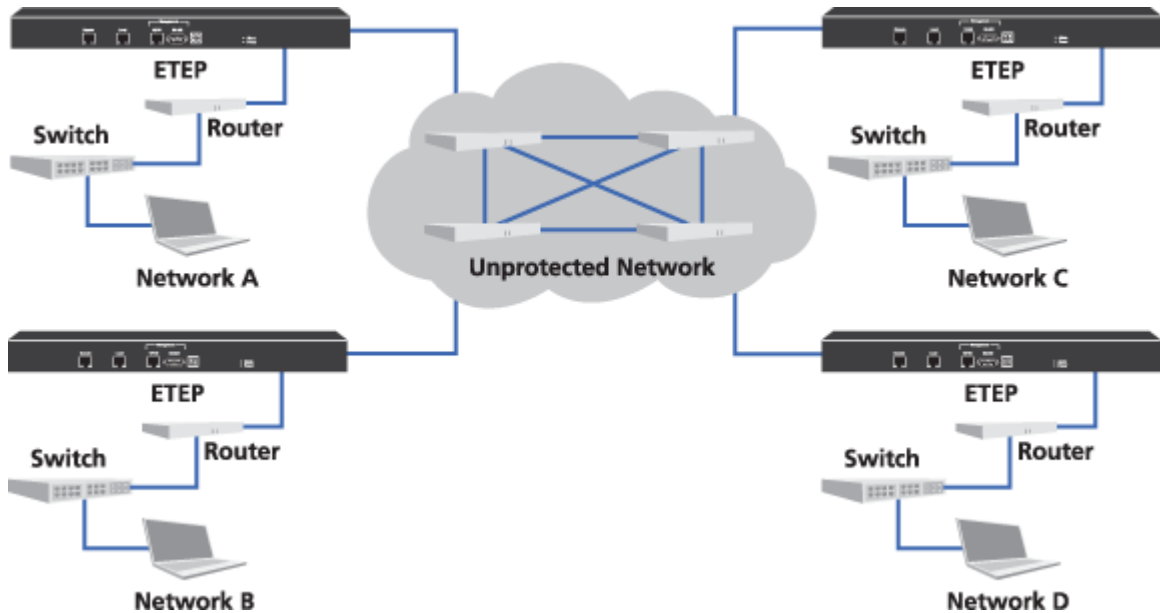
 **NOTE**

This option is only available for IPSec policies.

Adding Layer 2 Ethernet Policies

For Layer 2 Ethernet networks, policies can be created for mesh networks. In a mesh network, any network or network set can send or receive data from any other network or network set.

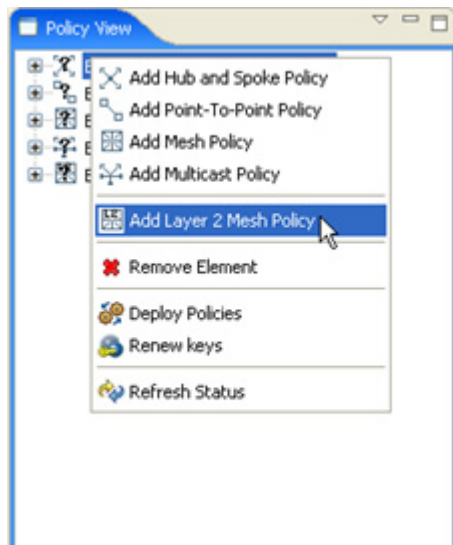
Figure 70 Mesh network example



The PEP for each network in [Figure 70](#) encrypts data sent to networks A, B, C, or D and decrypts data from networks A, B, C, or D.

To add a new Layer 2 mesh policy:

- 1 From the Policy view, right-click anywhere in the Policy view and click **Add Layer 2 Mesh Policy**.



- 2 Double click the new policy name added to the policy list.
- 3 Create the policy in the Mesh Policy editor as described in [Table 47](#). The policy editor is shown in [Figure 71](#).

4 Click **Save** when complete.

Table 47 Layer 2 Mesh policy entries

Field	Description
Name	Enter a unique name to identify the policy. Names can be 1 - 40 characters in length. Alphanumeric characters and spaces are valid. The special characters <, >, &, ", *, ?, /, \, : and cannot be used in the policy name. Names are not case sensitive.
Priority	Specifies the order in which policies are processed in the PEPs. Enter the priority for this policy from 1 to 65000. PEPs enforce policies in descending priority order with the highest priority number processed first.
Renew Keys/ Refresh Lifetime	Specifies the lifetime of the keys and policies, and the frequency at which the keys are regenerated and policies' lifetimes are updated on the PEPs. Regenerate keys and update policies either at a specified interval in hours or daily at a specified time. Click either Hours or Daily . <ul style="list-style-type: none"> • Hours - enter the re-key interval in hours between 0 and 65535 hours. 0 hours causes keys and policies to never expire and never update. Use 0 hours for drop and clear policy types. • Daily - enter the re-key time using the 24 hour system clock set to the required local time of the ETPM workstation. The re-key time will translate to the local times of the ETKMSs and PEPs that might be located in other time zones.
Type	Specifies the action applied to frames that match the protocol and networks included in this policy. <ul style="list-style-type: none"> • Drop - drops all frames matching this policy. • Bypass - passes all frames matching this policy in the clear. • Encrypt - encrypts or decrypts all frames matching this policy.
Protecting Policy Enforcement Points	Lists the PEPs where the policies and keys are distributed. Click the PEPs tab in the EncryptTight components view and drag the appropriate Layer 2 PEP to the PEPs list on the Policy editor. <ul style="list-style-type: none"> • You can also edit a PEP from this editor. Right-click the desired PEP and click Edit. • To remove a PEP from this list, right-click the desired PEP and click Remove Element. The PEP is removed only from this policy.
VLAN ID Ranges (optional)	Specifies a VLAN ID tag range for a policy. The policy affects only frames with a VLAN ID tag within the specified range. Traffic that does not match the VLAN ID tag (or range of tags) specified in the policy is dropped. If no range is specified, the policy applies to all frames. <p>EPEP PEPs accept only single VLAN ID tags in policies.</p> <p>Click the VLAN Ranges tab in the EncryptTight Components view and drag the appropriate VLAN range to the VLAN Ranges list on the Policy editor.</p> <ul style="list-style-type: none"> • You can also edit a VLAN Range from this editor. Right-click the desired VLAN Range and click Edit. • To remove a VLAN Range from this list, right-click the desired VLAN Range and click Remove Element. The VLAN range is removed only from this policy.
Key Generation and Distribution	Select the desired Key Management System from the ETKMS list.

Figure 71 Layer 2 Mesh policy editor

Layer 2 Mesh Policy

Name: Layer2Mesh: 65000

Priority: 65000

Renew keys/Refresh lifetime

Hours: 24 Daily: 12:01

Type

Drop Bypass Encrypt

Protecting Policy Enforcement Points

PEPS:

PEPS	
Branch A	
Branch B	
Headquarters	

VLAN ID Range

VLAN IDs:

Lower ID	Upper ID	Name

Key Generation and Distribution

ETKMS: Main

Save Cancel

NOTE

If you need to encrypt or pass in the clear specific routing protocols, consider also creating local site policies. Local site policies allow you to create locally configured policies using CLI commands, without requiring an EncryptTight ETKMS for key distribution. The primary use for local site policies is to facilitate in-line management in Layer 2 encrypted networks. These policies supplement existing encryption policies, adding the flexibility to encrypt or pass in the clear specific Layer 3 routing protocols, or Layer 2 Ethertypes and VLAN IDs. For information on creating and using local site policies, see the CLI User Guide.

Adding Layer 3 IP Policies

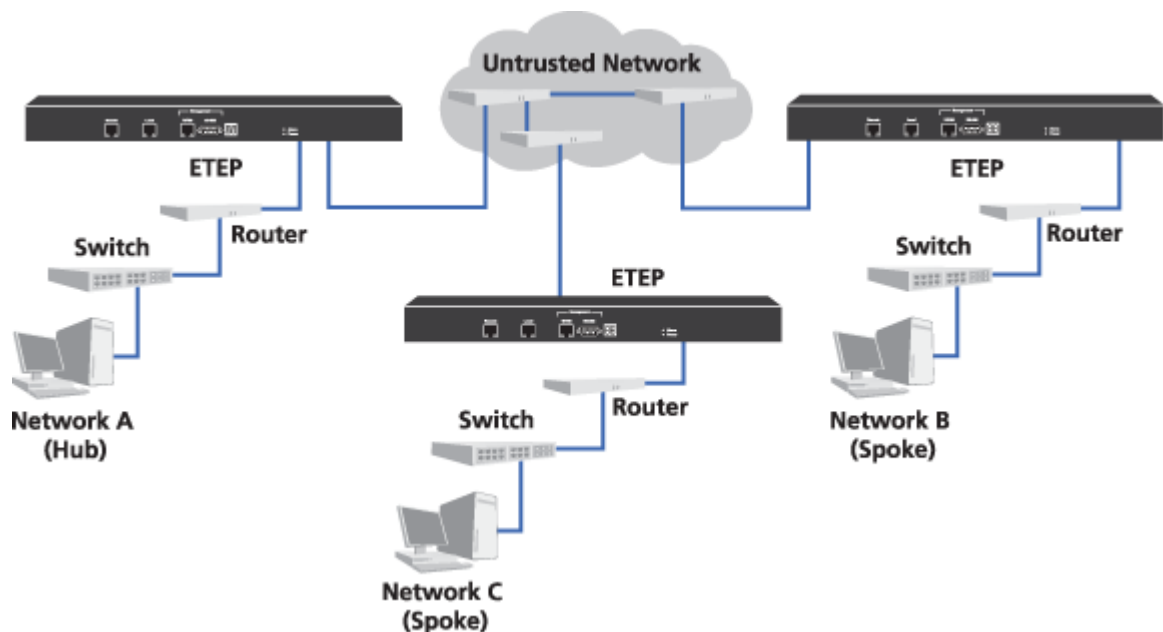
An IP policy can be created for hub and spoke, mesh, multicast, and point-to-point networks.

- [Adding a Hub and Spoke Policy](#)
- [Adding a Mesh Policy](#)
- [Adding a Multicast Policy](#)
- [Adding a Point-to-point Policy](#)

Adding a Hub and Spoke Policy

In a hub and spoke network, all transmissions either originate from a hub network and are received by a spoke network or originate from one of the spoke networks and are received by the hub network.

Figure 72 Secured hub and spoke example

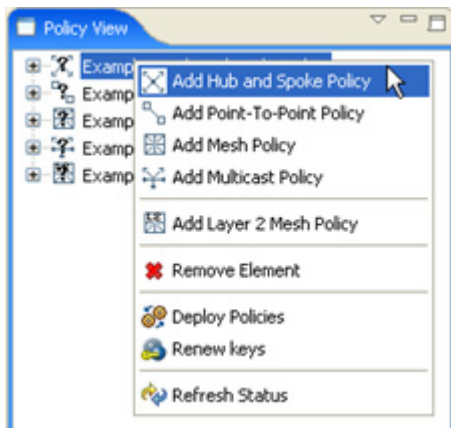


- PEP A encrypts data traffic from network A that goes to Networks B or C. PEP A also decrypts data that originates from Network B and C.
- PEP B encrypts data from network B that goes to network A and decrypts data that comes from network A.
- PEP C encrypts data from network C that goes to network A and decrypts data that comes from network A.
- PEP B and PEP C have no security associations to allow for decryption of traffic originating from each other.

When you create a policy for a hub and spoke network, you must select at least one hub network set and one spoke network set.

To add a new hub and spoke policy:

- 1 In the Policy view, right-click anywhere in the view and click **Add Hub and Spoke Policy**.



- 2 Double click the new policy name added to the policy list.
- 3 Create the policy in the Hub and Spoke Policy editor described in [Table 48](#). The policy editor is shown in [Figure 73](#).
- 4 Click **Save** when complete.

Table 48 Hub and spoke policy entries

Field	Description
Name	Enter a unique name to identify the policy. Names can be 1 - 40 characters in length. Alphanumeric characters and spaces are valid. The special characters <, >, &, " , * , ? , / , \ , : and cannot be used in the policy name. Names are not case sensitive.
Priority	Enter the priority for this policy from 1 to 65000. PEPs enforce policies in descending priority order with the highest priority number processed first.
Renew Keys/ Refresh Lifetime	Specifies the lifetime of the keys and policies, and the frequency at which the keys are regenerated and the policies' lifetimes are updated on the PEPs. Regenerate keys and update policies either at a specified interval in hours or daily at a specified time. Click either Hours or Daily . <ul style="list-style-type: none"> • Hours - enter the re-key interval in hours between 0 and 65535 hours. 0 hours causes keys and policies to never expire and never update. Use 0 hours for drop and clear policy types. • Daily - enter the re-key time using the 24 hour system clock set to the required local time of the ETPM workstation. The re-key time will translate to the local times of the ETKMSs and PEPs that might be located in other time zones.
Type	Specifies the action applied to packets that match the protocol and networks included in this policy. <ul style="list-style-type: none"> • Drop - drops all packets matching this policy. • Bypass - passes all packets matching this policy in the clear. • IPSec - encrypts or decrypts all packets matching this policy.

Table 48 Hub and spoke policy entries (continued)

Field	Description
IPSec	<p>Specifies the encryption and authentication algorithms used in an IPSec policy. Select the encryption algorithm from the Encryption Algorithms list:</p> <ul style="list-style-type: none"> • AES - Advanced Encryption Standard (default) • 3DES - a more secure variant of Data Encryption Standard <p>Select the authentication algorithm from the Authentication Algorithms list:</p> <ul style="list-style-type: none"> • HMAC-SHA-1 - Secure Hash Algorithm • HMAC-MD5 - Message Digest 5 <p>Note: Layer 4 policies require AES and HMAC-SHA-1.</p>
Key Generation	<p>Specifies the key generation and distribution mechanism for the PEPs included in the policy.</p> <ul style="list-style-type: none"> • By Network Set - The default ETKMS within each network set generates and distributes the keys to the PEPs included in those network sets. • Global ETKMS - A global ETKMS generates the keys and sends them to the default ETKMSs in each network set for distribution to all of PEPs included in the policy. <p>Select the desired ETKMS from the Global ETKMS list.</p>
Addressing Mode Override	<p>Overrides the Network addressing setting for the network sets.</p> <ul style="list-style-type: none"> • Preserve internal network addresses - This setting overrides the network set's network addressing mode and preserves the network addressing of the protected networks. The IP header contains the source address of the originating network. <p>If this setting is disabled and the addressing mode of the network set uses the PEP's remote IP address or a Virtual IP address, the IP header contains the source address as specified in the network set. If the addressing mode of the network set preserves the network IP address, disabling this setting has no effect.</p> <ul style="list-style-type: none"> • Preserve address, protocol and port - This setting overrides the network set's addressing mode and preserves the network addressing of the protected networks, as well as the specified protocol and port numbers. The IP header includes the source address, protocol, and port of the originating network. This allows you to send the Layer 4 header information in the clear for traffic engineering and Service Level Agreement (SLA) management (for example, Quality of Service controls).
Minimize Policy Size	<p>Reduces policy size by ignoring the network addresses on the local port of the PEP. This reduces the amount of network traffic needed to renew keys and refresh policy lifetimes.</p> <ul style="list-style-type: none"> • Minimize Policy Size (ignore source IP address) - This setting replaces the source network address for outbound traffic and the destination network address for inbound traffic with all networks wildcard addresses (0.0.0.0/0). For more information, see "Minimizing Policy Size" on page 187.
Network Sets	<p>Identifies the network sets included in this policy.</p> <p>Click the Network Sets tab of the EncryptTight Components view and drag the appropriate network sets to either Hubs or Spokes.</p>
Protocol	<p>Specifies the Layer 3 protocol affected by this policy. The action selected for the policy is only applied to the traffic with the specified protocol.</p> <ul style="list-style-type: none"> • Any - specifies all protocols • Only - specifies a particular protocol. Click to select and then enter the required protocol in the range 0 to 255.

Figure 73 Hub and spoke policy editor

Hub-Spoke Policy

Name:

Priority:

Renew keys/Refresh lifetime

Hours: Daily:

Type

Drop Bypass IPsec

IPsec

Encryption Algorithm:

Authentication Algorithm:

Key Generation

By NetworkSet Global ETKMS:

Addressing Mode Override

Preserve internal network addresses

Preserve address, protocol and port

Minimize Policy Size

Minimize Policy Size (ignore source IP address)

Network Sets

Hubs	
Network Sets:	
Main Office	

Spokes	
Network Sets:	
Cary	
Durham	

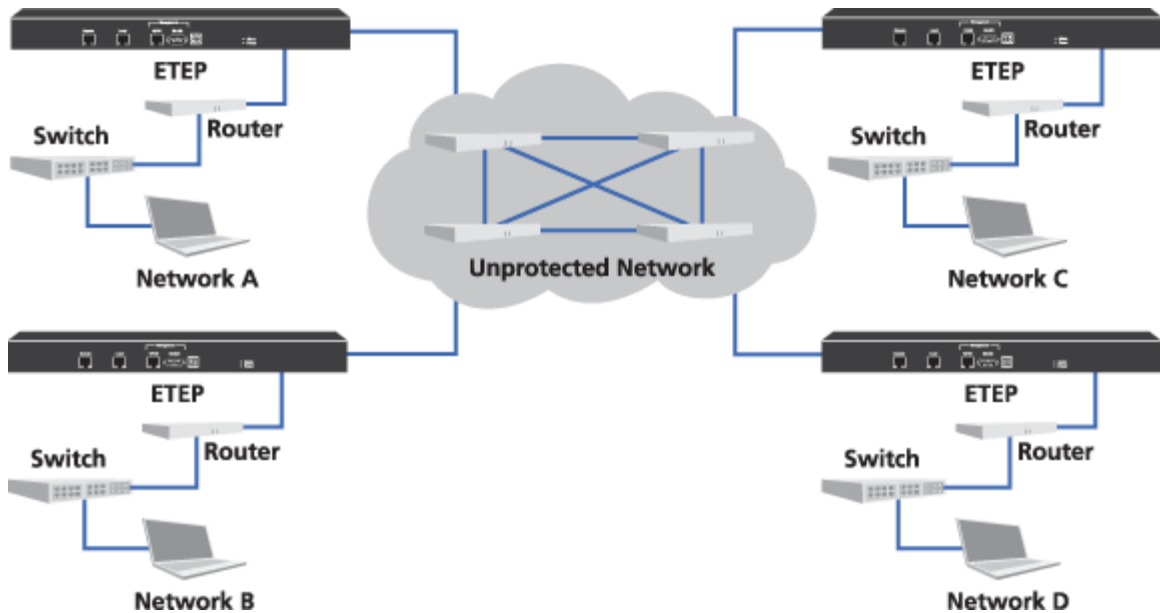
Protocol

Any Only:

Adding a Mesh Policy

In a mesh network, any network or network set can send or receive data from any other network or network set.

Figure 74 Mesh network example

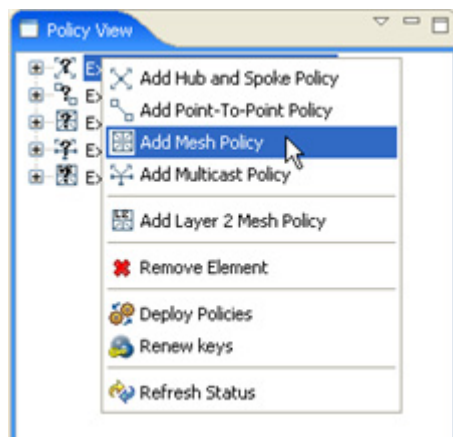


The PEP for each network in [Figure 74](#) encrypts data sent to networks A, B, C, or D and decrypts data from networks A, B, C, or D.

When you create a policy for a Mesh network, you must select at least two network sets.

To add a new mesh policy:

- 1 From the Policy view, right-click anywhere in the Policy view and click **Add Mesh Policy**.



- 2 Double click the new policy name added to the policy list.
- 3 Create the policy in the Mesh Policy editor as described in [Table 49](#). The policy editor is shown in [Figure 75](#).
- 4 Click **Save** when complete.

Table 49 Mesh policy entries

Field	Description
Name	Enter a unique name to identify the policy. Names can be 1 - 40 characters in length. Alphanumeric characters and spaces are valid. The special characters <, >, &, "*", ?, /, \, : and cannot be used in the policy name. Names are not case sensitive.
Priority	Enter the priority for this policy from 1 to 65000. PEPs enforce policies in descending priority order with the highest priority number processed first.
Renew Keys/ Refresh Lifetime	Specifies the lifetime of the keys and policies, and the frequency at which the keys are regenerated and policies' lifetimes are updated on the PEPs. Regenerate keys and update policies either at a specified interval in hours or daily at a specified time. Click either Hours or Daily . <ul style="list-style-type: none"> • Hours - enter the re-key interval in hours between 0 and 65535 hours. 0 hours causes keys and policies to never expire and never update. Use 0 hours for drop and clear policy types. • Daily at - enter the re-key time using the 24 hour system clock set to the required local time of the ETPM workstation. The re-key time will translate to the local times of the ETKMSs and PEPs that might be located in other time zones.
Type	Specifies the action applied to packets that match the protocol and networks included in this policy. <ul style="list-style-type: none"> • Drop - drops all packets matching this policy. • Bypass - passes all packets matching this policy in the clear. • IPSec - encrypts or decrypts all packets matching this policy.
IPSec	Specifies the encryption and authentication algorithms used in an IPSec policy. Select the encryption algorithm from the Encryption Algorithms list: <ul style="list-style-type: none"> • AES - Advanced Encryption Standard (default) • 3DES - a more secure variant of Data Encryption Standard Select the authentication algorithm from the Authentication Algorithms list: <ul style="list-style-type: none"> • HMAC-SHA-1 - Secure Hash Algorithm • HMAC-MD5 - Message Digest 5 Note: Layer 4 policies require AES and HMAC-SHA-1.
Key Generation	Specifies the key generation and distribution mechanism for the PEPs included in this policy. <ul style="list-style-type: none"> • By Network Set - The default ETKMS within each network set generates and distributes the keys to the PEPs included in those network sets. • Global ETKMS - A global ETKMS generates the keys and sends them to the default ETKMSs in each network set for distribution to all of PEPs included in the policy. Select the desired ETKMS from the Global ETKMS list.

Table 49 Mesh policy entries (continued)

Field	Description
Addressing Mode Override	<p>Overrides the Network addressing setting for the network sets.</p> <ul style="list-style-type: none"> • Preserve internal network addresses - This setting overrides the network set's network addressing mode and preserves the network addressing of the protected networks. The IP header contains the source address of the originating network. If this setting is disabled and the addressing mode of the network set uses the PEP's remote IP address or a Virtual IP address, the IP header contains the source address as specified in the network set. If the addressing mode of the network set preserves the network IP address, disabling this setting has no effect. • Preserve address, protocol and port - This setting overrides the network set's addressing mode and preserves the network addressing of the protected networks, as well as the specified protocol and port numbers. The IP header includes the source address, protocol, and port of the originating network. This allows you to send the Layer 4 header information in the clear for traffic engineering and Service Level Agreement (SLA) management (for example, Quality of Service controls).
Minimize Policy Size	<p>Specifies a method for reducing the policy size.</p> <ul style="list-style-type: none"> • Ignore source IP address - Reduces policy size by ignoring the network addresses on the local port of the PEP. This limits the amount of network traffic needed to renew keys and refresh policy lifetimes. If you select this option, the source network address for outbound traffic and the destination network address for inbound traffic are replaced with all networks wildcard addresses (0.0.0.0/0). • Apply to all traffic - Reduces the policy size by applying the policy to all traffic, inbound and outbound, regardless of the source and destination address and ports. If the policy specifies encryption, all PEPs associated with the policy use the same key set. This option reduces the number of policy entries and SAs on each PEP. <p>For more information, see "Minimizing Policy Size" on page 187.</p>
Network Sets	<p>Identifies the network sets included in this policy.</p> <p>Click the Network Sets tab of the EncrypTight Components view and drag the appropriate network sets to Mesh Network Sets.</p>
Protocol	<p>Specifies the Layer 3 protocol affected by this policy. The action selected for the policy is only applied to the traffic with the specified protocol.</p> <ul style="list-style-type: none"> • Any - specifies all protocols. • Only - specifies a particular protocol. Click to select and then enter the required protocol in the range 0 to 255.

Figure 75 Mesh policy editor

The screenshot shows the 'New Mesh Policy 17: 65000' dialog box with the following configuration:

- Mesh Policy:** Name: New Mesh Policy 17: 65000, Priority: 65000
- Renew keys/Refresh lifetime:** Hours: 24 (selected), Daily: 12:01
- Type:** Drop, Bypass, IPsec (selected)
- IPSec:** Encryption Algorithm: AES, Authentication Algorithm: HMAC-SHA-1
- Key Generation:** By NetworkSet (selected), Global ETKMS: Main
- Addressing Mode Override:** Preserve internal network addresses (checked), Preserve address, protocol and port (unchecked)
- Minimize Policy Size:** Ignore source IP address (unchecked), Apply to all traffic (unchecked)
- Network Sets:**

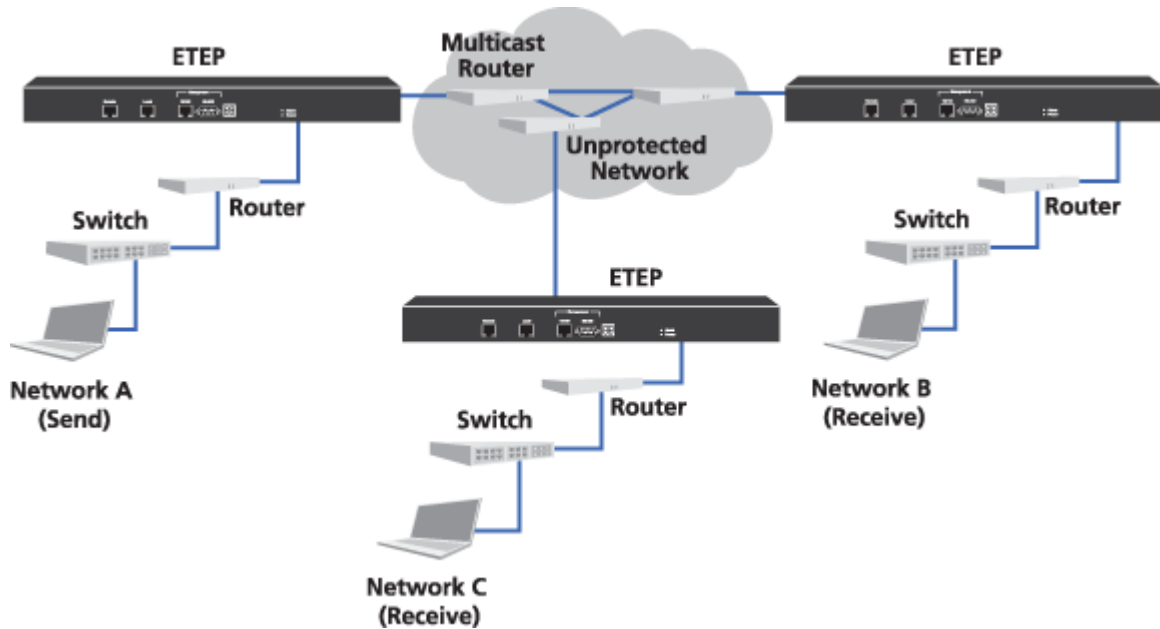
Mesh NetworkSets:	
Network Set 1	
Network Set 2	
- Protocol:** Any (selected), Only: 0

Buttons: Save, Cancel

Adding a Multicast Policy

In a multicast network, one or more networks send unidirectional streams to multiple destination networks. The multicast routers detect the multicast transmission, determine which nodes have joined the multicast network as destination networks and duplicate the packet as needed to reach all multicast destination networks.

Figure 76 Multicast network example

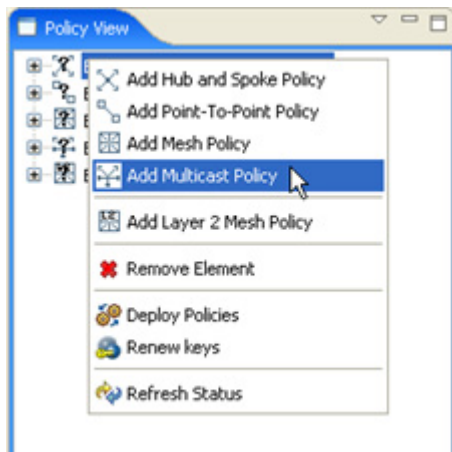


The policy for the example in [Figure 76](#) specifies Network A as the send network. This policy also specifies networks B and C as the destination or receive networks. Networks B and C are set up in the multicast routers as members of the multicast network. PEP 1 encrypts multicast traffic sent from Network A to the multicast IP address. PEPs 2 and 3 decrypt data received at Network B and C that originates from the multicast network IP address.

When you create a multicast policy, you must select a ETKMS and specify a multicast network IP address. At least one network set must be selected as either send only or send and receive, and at least one network set must be selected as either receive only or send and receive.

To add a multicast policy:

- 1 In the Policy view, right-click anywhere in the view and click **Add Multicast Policy**.



- 2 Double click the new policy name added to the policy list.
- 3 Create the policy in the Multicast Policy editor as described in [Table 50](#). The policy editor is shown in [Figure 77](#).
- 4 Click **Save** when complete.

Table 50 Multicast policy entries

Field	Description
Name	Enter a unique name to identify the policy. Names can be 1 - 40 characters in length. Alphanumeric characters and spaces are valid. The special characters <, >, &, " , * , ? , / , \ , : and cannot be used in the policy name. Names are not case sensitive.
Priority	Enter the priority for this policy from 1 to 65000. PEPs enforce policies in descending priority order with the highest priority number processed first.
Renew Keys/ Refresh Lifetime	Specifies the lifetime of the keys and policies, and the frequency at which the keys are regenerated and policies' lifetimes are updated on the PEPs. Regenerate keys and update policies either at a specified interval in hours or daily at a specified time. Click either Hours or Daily . <ul style="list-style-type: none"> • Hours - enter the re-key interval in hours between 0 and 65535 hours. 0 hours causes keys and policies to never expire and never update. Use 0 hours for drop and clear policy types. • Daily - enter the re-key time using the 24 hour system clock set to the required local time of the ETPM workstation. The re-key time will translate to the local times of the ETKMSs and PEPs that might be located in other time zones.
Type	Specifies the action applied to packets that match the protocol and networks included in this policy. <ul style="list-style-type: none"> • Drop - drops all packets matching this policy. • Bypass - passes all packets matching this policy in the clear. • IPSec - encrypts or decrypts all packets matching this policy.

Table 50 Multicast policy entries (continued)

Field	Description
IPSec	<p>Specifies the encryption and authentication algorithms used in an IPSec policy. Select the encryption algorithm from the Encryption Algorithms list:</p> <ul style="list-style-type: none"> • AES - Advanced Encryption Standard (default) • 3DES - a more secure variant of Data Encryption Standard <p>Select the authentication algorithm from the Authentication Algorithms list:</p> <ul style="list-style-type: none"> • HMAC-SHA-1 - Secure Hash Algorithm • HMAC-MD5 - Message Digest 5 <p>Note: Layer 4 policies require AES and HMAC-SHA-1.</p>
Key Generation	<p>Specifies the global ETKMS used in the multicast network. A global ETKMS generates the keys and sends them to the default ETKMSs in each network set for distribution to all of PEPs included in the policy. Select the desired ETKMS from the ETKMS list.</p>
Addressing Mode Override	<p>Overrides the Network addressing setting for the network sets.</p> <ul style="list-style-type: none"> • Preserve internal network addresses - This setting is always enabled for multicast policies and cannot be disabled. By default, multicast policies override network set's network addressing mode and preserve the network addressing of the protected networks. The IP header contains the source address of the originating network. • Preserve address, protocol and port - This setting overrides the network set's addressing mode and preserves the network addressing of the protected networks, as well as the specified protocol and port numbers. The IP header includes the source address, protocol, and port of the originating network. This allows you to send the Layer 4 header information in the clear for traffic engineering and Service Level Agreement (SLA) management (for example, Quality of Service controls).
Minimize Policy Size	<p>Reduces policy size by ignoring the network addresses on the local port of the PEP. This reduces the amount of network traffic needed to renew keys and refresh policy lifetimes.</p> <ul style="list-style-type: none"> • Minimize Policy Size (Ignore Source IP) - This setting replaces the source network address for outbound traffic with an all networks wildcard address (0.0.0.0/0). For more information, see "Minimizing Policy Size" on page 187.
Multicast Network	<p>Identifies the multicast address range protected by this policy.</p> <ul style="list-style-type: none"> • IP - multicast IP address • Mask - mask for the multicast IP address
Network Sets	<p>Identifies the networks included in this policy.</p> <p>Click on the Network Sets tab of the EncrypTight Components view and drag the appropriate network sets to the desired columns.</p> <ul style="list-style-type: none"> • Send - lists the networks that only send data • Receive - lists the networks that only receive data • Send and Receive - lists the networks that send and receive data <p>ETPM supports technologies such as Protocol Independent Multicast (PIM) by providing the ability to have multiple senders, receivers, and senders/receivers in multicast policies.</p>

Figure 77 Multicast policy editor

New Multicast Policy 41: 55000

Multicast Policy
 Name:
 Priority:

Renew keys/Refresh Lifetime
 Hours: Daily:

Type
 Drop Bypass IPsec

IPsec
 Encryption Algorithm:
 Authentication Algorithm:

Key Generation
 ETKMS:

Addressing Mode Override
 Preserve internal network addresses
 Preserve address, protocol and port

Minimize Policy Size
 Minimize Policy Size (ignore source IP address)

Multicast Network
 IP:
 Mask:

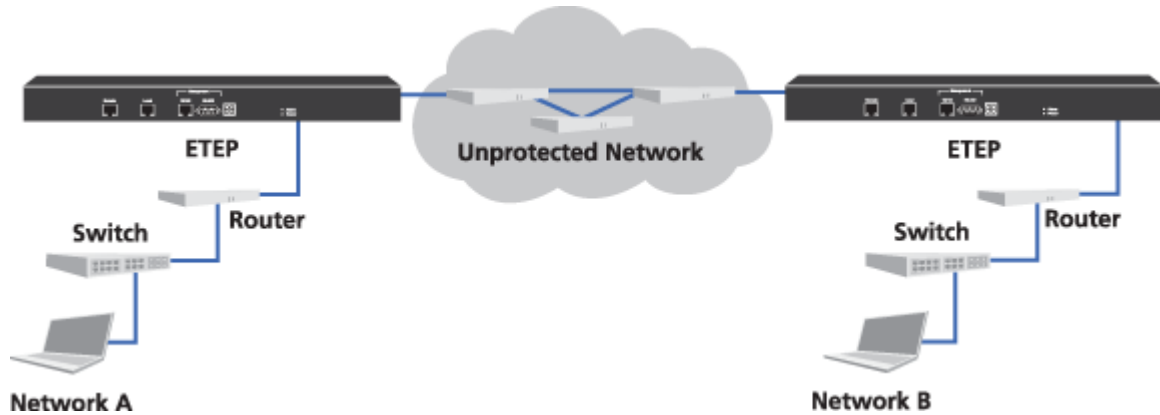
Network Sets

Send	Receive	Send/Receive
Network Sets: Main Office	Network Sets: Region2	Network Sets: Region 3
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

Adding a Point-to-point Policy

In a point-to-point network, one network or network set sends and receives data to and from one other network or network set.

Figure 78 Point-to-point network example

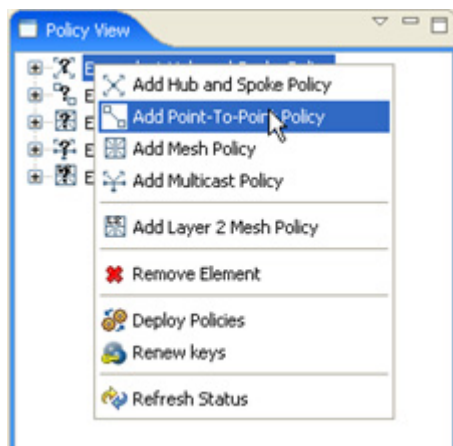


In [Figure 78](#), the end-points are Networks A and B. PEP 1 encrypts the traffic sent from Network A to Network B and decrypts traffic received from Network B. PEP 2 encrypts the traffic sent from Network B to Network A and decrypts traffic received from Network A.

When you create a point-to-point policy, you must select one network set for each point.

To add a point-to-point policy:

- 1 From the Policy view, right-click anywhere in the view and click **Add Point-To-Point Policy**.



- 2 Double click the new policy name added to the policy list.
- 3 Create the policy in the Point-to-Point Policy editor as described in [Table 51](#). The policy editor is shown in [Figure 79](#).

4 Click **Save** when complete.

Table 51 Point-to-point policy entries

Field	Description
Name	Enter a unique name to identify the policy. Names can be 1 - 40 characters in length. Alphanumeric characters and spaces are valid. The special characters <, >, &, " *, ?, /, \, : and cannot be used in the policy name. Names are not case sensitive.
Priority	Enter the priority for this policy from 1 to 65000. PEPs enforce policies in descending priority order with the highest priority number processed first.
Renew Keys/ Refresh Lifetime	Specifies the lifetime of the keys and policies, and the frequency at which the keys are regenerated and policies' lifetimes are updated on the PEPs. Regenerate keys and update policies either at a specified interval in hours or daily at a specified time. Click either Hours or Daily . <ul style="list-style-type: none"> • Hours - enter the re-key interval in hours between 0 and 65535 hours. 0 hours causes keys and policies to never expire and never update. Use 0 hours for drop and clear policy types. • Daily - enter the re-key time using the 24 hour system clock set to the required local time of the ETPM workstation. The re-key time will translate to the local times of the ETKMSs and PEPs that might be located in other time zones.
Type	Specifies the action applied to packets that match the protocol and networks included in this policy. <ul style="list-style-type: none"> • Drop - drops all packets matching this policy. • Bypass - passes all packets matching this policy with no encryption and authentication. • IPSec - encrypts or decrypts all packets matching this policy.
IPSec	Specifies the encryption and authentication algorithms used in an IPSec policy. Select the encryption algorithm from the Encryption Algorithms list: <ul style="list-style-type: none"> • AES - Advanced Encryption Standard (default) • 3DES - a more secure variant of Data Encryption Standard Select the authentication algorithm from the Authentication Algorithms list: <ul style="list-style-type: none"> • HMAC-SHA-1 - Secure Hash Algorithm • HMAC-MD5 - Message Digest 5 Note: Layer 4 policies require AES and HMAC-SHA-1.
Key Generation	Specifies the key generation and distribution mechanism for the PEPs included in this policy. <ul style="list-style-type: none"> • By Network Set - The default ETKMS within each network set generates and distributes the keys to the PEPs included in those network sets. • Global ETKMS - A global ETKMS generates the keys and sends them to the default ETKMSs in each network set for distribution to all of PEPs included in the policy. Select the desired ETKMS from the Global ETKMS list.

Table 51 Point-to-point policy entries (continued)

Field	Description
Addressing Mode Override	<p>Overrides the Network addressing setting for the network sets.</p> <ul style="list-style-type: none"> • Preserve internal network addresses - This setting overrides the network set's network addressing mode and preserves the network addressing of the protected networks. The IP header contains the source address of the originating network. If this setting is disabled and the addressing mode of the network set uses the PEP's remote IP address or a Virtual IP address, the IP header contains the source address as specified in the network set. If the addressing mode of the network set preserves the network IP address, disabling this setting has no effect. • Preserve address, protocol and port - This setting overrides the network set's addressing mode and preserves the network addressing of the protected networks, as well as the specified protocol and port numbers. The IP header includes the source address, protocol, and port of the originating network. This allows you to send the Layer 4 header information in the clear for traffic engineering and Service Level Agreement (SLA) management (for example, Quality of Service controls).
Minimize Policy Size	<p>Reduces policy size by ignoring the network addresses on the local port of the PEP. This reduces the amount of network traffic needed to renew keys and refresh policy lifetimes.</p> <ul style="list-style-type: none"> • Minimize Policy Size (Ignore Source IP) - This setting replaces the source network address for outbound traffic and the destination network address for inbound traffic with all networks wildcard addresses (0.0.0.0/0). For more information, see "Minimizing Policy Size" on page 187.
Point A - Network Set	<p>Identifies the network set included in this policy for one side of the point-to-point network configuration.</p> <ul style="list-style-type: none"> • Click the Network Sets tab of the EncrypTight Components view and drag the appropriate network set to the Point A - Network Set.
Point A - Ports	<p>Specifies the source and destination ports for the network set selected for Point A. In TCP and UDP, port numbers are used to identify well-known services, such as FTP, e-mail and so on. Choosing a specific port limits the action of the policy to traffic using that port.</p> <p>This setting is only valid if the protocol is set to 6 (TCP) or 17 (UDP).</p>
Point B - Network Set	<p>Identifies the network set included in this policy for the other side of the point-to-point network configuration.</p> <ul style="list-style-type: none"> • Click on the Network Sets tab of the EncrypTight Components view and drag the appropriate network set to the Point B - Network Set menu.
Point B - Ports	<p>Specifies the source and destination ports for the network set selected for Point B. In TCP and UDP, port numbers are used to identify well-known services, such as FTP, e-mail and so on. Choosing a specific port limits the action of the policy to traffic using that port.</p> <p>This setting is only valid if the protocol is set to 6 (TCP) or 17 (UDP).</p>
Protocol	<p>Specifies the Layer 3 protocol affected by this policy. The action selected for the policy is only applied to the traffic with the specified protocol.</p> <ul style="list-style-type: none"> • Any - specifies all protocols • Only - specifies a particular protocol. Click to select and then enter the required protocol in the range 0 to 255.

Figure 79 Point-to-point policy editor

Adding Layer 4 Policies

Layer 4 policies encrypt only the payload of the packet. The source and destination addresses, protocol, and port in the IP header are sent in the clear. With Layer 4 policies, the Layer 4 header information is sent in the clear for traffic engineering and Service Level Agreement management (for example, Quality of Service controls or NetFlow statistics monitoring). You can create Layer 4 policies for point-to-point, hub and spoke, mesh, and multicast network topologies.

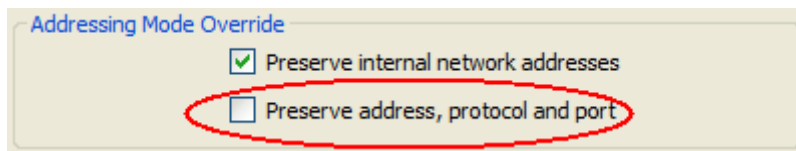
You create Layer 4 policies using ETEPs that are configured to operate as Layer 3 PEPs. Create the networks, network sets, and policies as you would for Layer 3 IP policies. In the policy editor, select the option to preserve the address, protocol, and port. This option encrypts only the payload data, making the policy a Layer 4 policy.

Layer 4 IP encryption policies use AES-256 for encryption and HMAC-SHA-1 for authentication. The ETEP PEPs do not support 3DES or HMAC-MD5 at Layer 4.

To create a new Layer 4 policy:

- 1 Right click anywhere in the policy view and select an IP policy type from the shortcut menu.
- 2 Follow the instructions for creating the type of policy you selected as discussed in [“Adding Layer 3 IP Policies”](#) on page 191.
- 3 From the Addressing Mode Override section of the policy editor, select **Preserve address, protocol and port** (see [Figure 80](#)).
- 4 Save the policy.

Figure 80 Option to Encrypt the Packet Payload Only



Policy Deployment

This section includes the following topics:

- [“Verifying Policy Rules Before Deployment”](#) on page 207
- [“Deploying Policies”](#) on page 208
- [“Setting Deployment Confirmation Preferences”](#) on page 208

Verifying Policy Rules Before Deployment


The Verify Policies tool checks your policies for conformance to the policy rules prior to deployment. This tool performs the same consistency checks on policies that are performed during a deploy operation. It differs from the deployment verification in that it does not check communication links to the ETKMS.

The Verify Policies tool checks for features that are not universally supported across PEP models and software versions. It looks for inconsistencies such as using a mixture of Layer 2 and Layer 3 PEPs in a policy, using contiguous and non-contiguous network masks in a network set, and the use of virtual IP addresses.

Verifying policies prior to deployment is useful if you have done any of the following:


- Made edits to any policy element since you last deployed policies: PEPs, networks, network sets, or policy definitions.
- The PEPs in a policy are running a mix of software versions, for example ETEPs running versions 1.4, 1.5, and 1.6.

To verify policies:

- 1 Click **Tools > Verify policies**. ETPM displays a confirmation message indicating the results of the rules check.
- 2 If the policies contain errors, go to the Policy View to locate them. Expand the policy tree to find the component with the configuration error. Double-click the component with the error to view the editor and find the entry with the configuration error. You can mouse over the  to view a message describing the error.


Deploying Policies

Policy deployment is the distribution of policies created in the Policy Manager (ETPM) to the appropriate Key Management Systems (ETKMSs) which in turn generate the keys and distribute the policies to the appropriate Policy Enforcement Points (PEPs).


Once the policies have been created and saved, deploy the policies by clicking  **Deploy**. Note that you cannot selectively deploy a specific policy. When you click **Deploy**, all policies are sent to the ETKMSs.

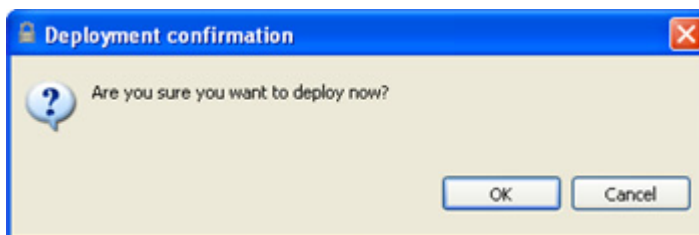
As soon as you deploy the policies, the Policy view status indicators change to yellow momentarily. Once the policies are successfully deployed, the status indicators change to green. For more information on status indicators, see [Table 37](#).

When you deploy policies, any errors cause the entire deployment to fail. No policies are deployed to the ETKMSs even if only one policy has an error.

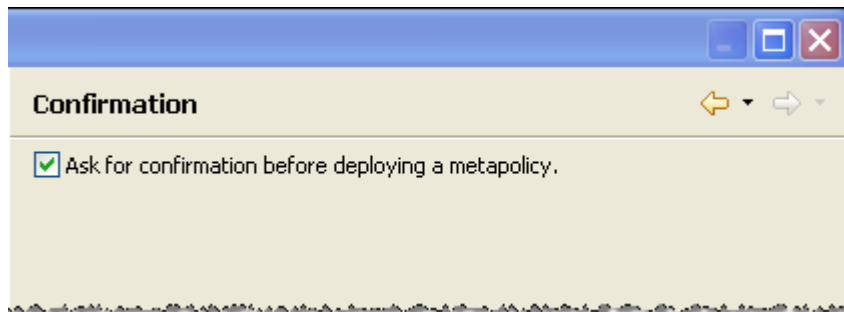
You cannot deploy policies that contain configuration errors in any of the policy components. If you attempt to do so, an error message appears with the text: “Policy Deployment is not allowed while configuration errors exist.” Expand the policy tree to locate the component with the configuration error. Double-click the component with the error to view the editor and find the entry with the configuration error. You can mouse over the  to view a message describing the error. Correct the problem and then retry.

Setting Deployment Confirmation Preferences

Since the deployment of policies can cause a brief interruption of traffic on the PEPs’ data ports, the ETPM displays a confirmation each time you click **Deploy** . You can disable this prompt.

**To enable or disable the deployment warning:**

- 1 From the ETPM main menu bar, click **Edit > Preferences**.
- 2 In the Preferences window, expand the ETPM listing and select **Confirmation**.

Figure 81 ETPM Preferences

- 3 Select or clear the **Ask for confirmation before deploying a metapolicy** checkbox.
- 4 Click **Apply**.

Editing a Policy

To edit an existing policy:

- 1 From the Policy view, double click the desired policy name on the policy list.
- 2 Modify the desired entries in the Policy editor.
- 3 Click **Save** on the Policy editor when complete.

NOTE


If one or more policies have been changed or added and the policies have not been deployed since the policy changes, the policy and PEP statuses display an  inconsistent indication.


Table 52 Editing policies

For information on the entries in a:	Refer to:
Layer 3/Layer 4 Hub and Spoke Policy	Table 48 on page 192
Layer 3/Layer 4 Mesh Policy	Table 49 on page 196
Layer 3/Layer 4 Multicast Policy	Table 50 on page 200
Layer 3/Layer 4 Point-to-point Policy	Table 51 on page 204
Layer 2 Mesh Policy	Table 47 on page 189

Deleting Policies

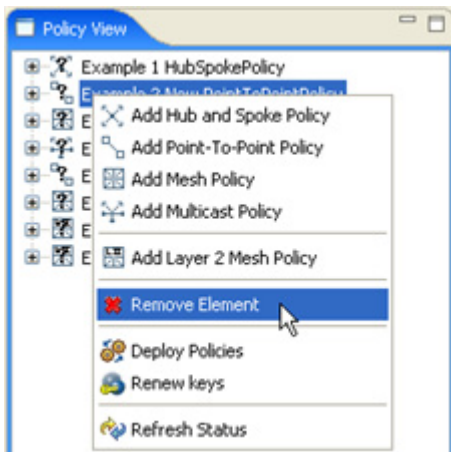
Security needs can change and in addition to editing policies, you can delete policies that are no longer needed.

NOTE

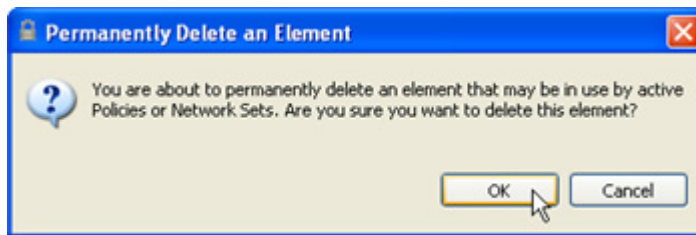
*Once the policy is deleted, the policy is removed from the ETPM's database but it continues running on all of the PEPs until you click  **Deploy**.*

To delete an existing policy:

- 1 From the Policy view, right-click the desired policy name and click **Remove element**.



- 2 Click **OK** on the Permanently Delete an Element window.



In addition to deleting specific policies, you can delete all of the policies on the ETEP. This can be useful in troubleshooting situations or if you need to relocate the ETEP. Clearing all policies from the ETEP restores the default policy to send all traffic in the clear.

To delete all policies:

- 1 In the Appliance Manager, select the ETEP.
- 2 Select **Tools > Clear Policies**.

 **NOTE**

You can also log into the CLI for the ETEP and use the `clear-policies` command to remove all policies. For more information, see [“Placing PEPs in Bypass Mode” on page 246](#) and the [ETEP CLI User Guide](#).

16 Policy Design Examples

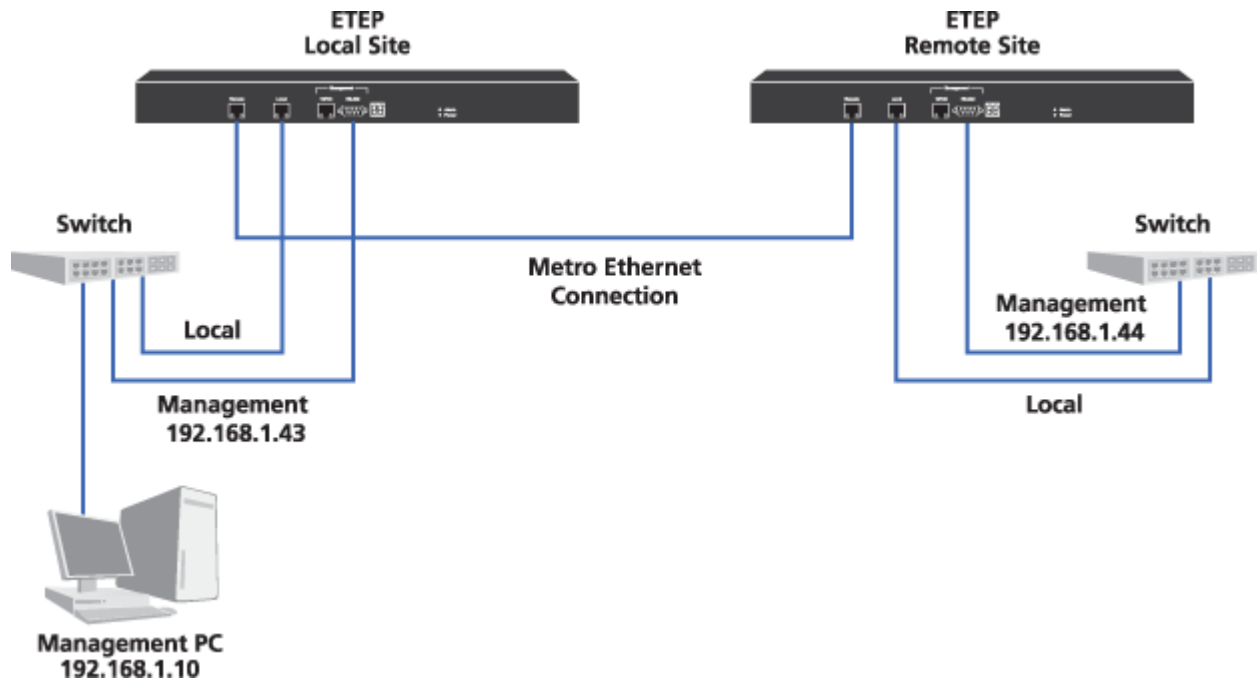
This section provides two examples of creating policies with EncrypTight:

- [Basic Layer 2 Point-to-Point Policy Example](#)
- [Layer 2 Ethernet Policy Using VLAN IDs](#)
- [Complex Layer 3 Policy Example](#)

Basic Layer 2 Point-to-Point Policy Example

In this example, we secure a single point-to-point Layer 2 Ethernet link using only the ETEMS software and two encryption appliances. This example focuses on the required settings and does not discuss advanced and optional settings.

Figure 82 Point-to-point Layer 2 Ethernet link



The requirement for this policy is to encrypt all traffic between the two points.

In ETEMS, configure the interfaces for both PEPs, then click the Features tab and do the following:

- 1 Select **Layer 2:Ethernet** for the Encryption Policy Settings.
- 2 Clear the **Enable EncrypTight** checkbox.

To set up the encryption policy between the two PEPs, click the Policy tab for each PEP and make the selections as described in [Table 53](#). Make sure that you use the same key for both PEPs.

Table 53 Point-to-point Layer 2 encryption policy

Setting	PEP: 192.168.1.43	PEP: 192.168.1.44
Role	Primary	Secondary
IKE Authentication Method	PresharedKey	PresharedKey
IKE Preshared Key	zaq123edc	zaq123edc
Group ID	0	0
Traffic Handling	EthEncrypt	EthEncrypt

Once the PEP configurations have been saved, push the configuration to the remote PEP first, and then push the configuration to the local PEP. For more information about creating Layer 2 point-to-point policies, see the Configuration chapter for your PEPs.

Layer 2 Ethernet Policy Using VLAN IDs

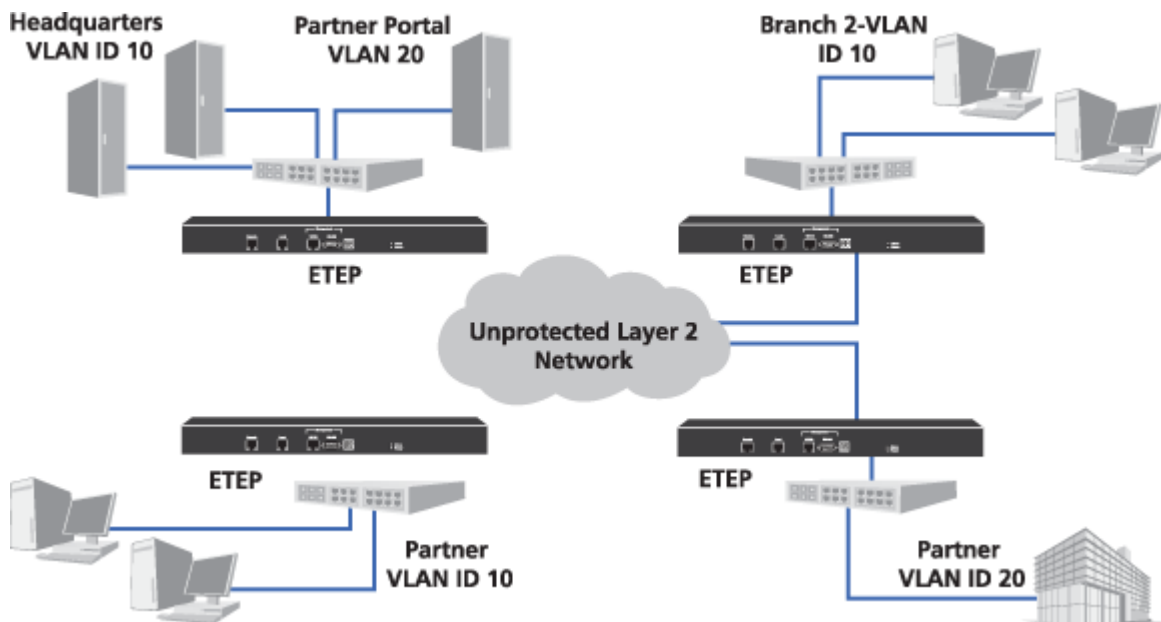
This example shows a more complicated Layer 2 Ethernet policy encrypting traffic using specific VLAN IDs. [Figure 83](#) shows a collection of networks for a company with a central headquarters and two branch offices. The company has a partner that needs access to specific company data, but does not need access to the branch offices.

Traffic between the headquarters and the branches is assigned a VLAN ID tag. This assures that communications between headquarters and the branches are not accidentally broadcast to other parties, such as the partner. Meanwhile, traffic between the partner and the partner portal server is assigned a different VLAN ID tag.

Finally, for added security all traffic not using one of the designated VLAN ID tags is discarded.

In this case, three separate policies need to be created:

- One Layer 2 Mesh encryption policy for traffic between the headquarters and each individual branch using VLAN ID 10
- One encryption policy for the traffic between the partner and partner portal server, using VLAN ID 20
- One drop policy that discards all traffic not using one of the specified VLAN ID tags, which is assigned a lower priority than the other policies

Figure 83 Using VLAN IDs**Policy Details****Policy 1: Headquarters and Branches**

Name: HQ/Branch Communications
Priority: 60000
Renew: Once every 24 Hours
Type: Encrypt
PEPs: Headquarters, Branch 1, Branch 2
VLAN ID: 10
ETKMS: ETKMS1

Policy 2: Partner and Partner Portal Server

Name: Branch 2 Communications
Priority: 60000
Renew: Once every 24 Hours
Type: Encrypt
PEPs: Headquarters, Partner
VLAN ID: 20
ETKMS: ETKMS1

Policy 3: Discard All Other

Name: Drop
Priority: 20000
Renew: 0 Hours
Type: Drop
PEPs: All
VLAN ID: None
ETKMS: ETKMS1

For simplicity, this example uses a single ETKMS, but you could use multiple ETKMSs if needed.

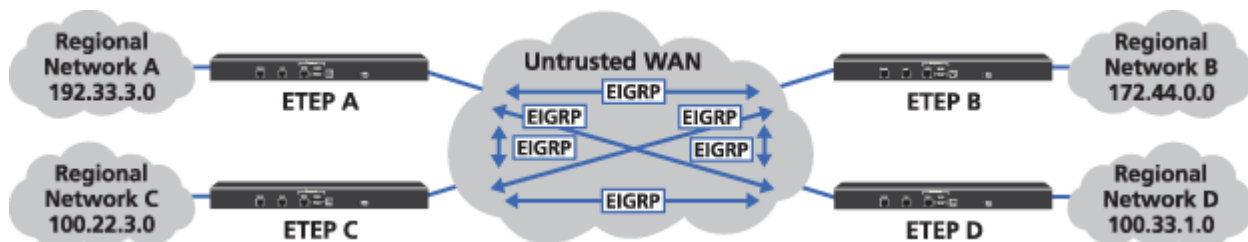
To create the policies:

- 1 In ETEMS, add and configure the ETEPs to operate as Layer 2 PEPs.
- 2 Add the ETKMS for the policies.
- 3 Push the configurations to the ETEPs.
- 4 In ETPM, add the VLAN ID tags.
- 5 Create the policies using the settings described in [“Policy Details” on page 213](#).
- 6 Deploy the policies.

Complex Layer 3 Policy Example

In this example, we have sixteen networks connecting to each other through a public WAN. Four of these networks are considered regional centers. Each regional center has three branches.

Figure 84 Network example



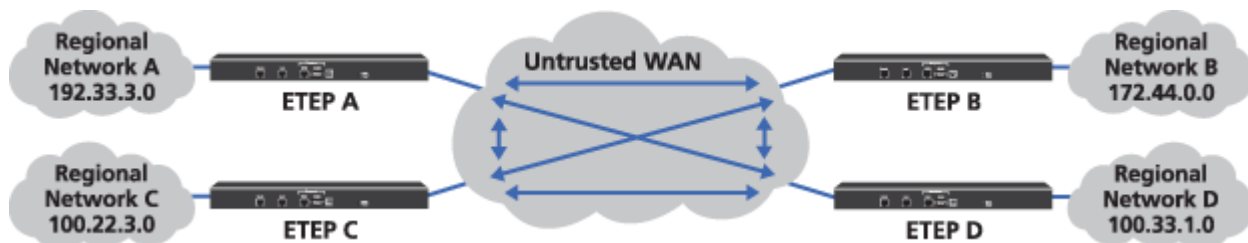
The requirements for our policies are as follows:

- [“Encrypt Traffic Between Regional Centers” on page 214](#)
- [“Encrypt Traffic Between Regional Centers and Branches” on page 215](#)
- [“Passing Routing Protocols” on page 218](#)

Encrypt Traffic Between Regional Centers

In order to encrypt traffic between the four regional centers, create a Mesh IPsec policy with each regional network in a different network set.

Figure 85 Regional mesh encryption policy



The network sets required for this policy are:

Table 54 Network sets for mesh policy

	Networks	PEPs	Default ETKMS
Network Set A	192.33.3.0 netmask 255.255.255.0	PEP A	ETKMS 1
Network Set B	172.44.0.0 netmask 255.255.255.0	PEP B	ETKMS 1
Network Set C	100.22.3.0 netmask 255.255.255.0	PEP C	ETKMS 1
Network Set D	100.33.1.0 netmask 255.255.255.0	PEP D	ETKMS 1

Using the four network sets, create the mesh policy as shown in the following table:

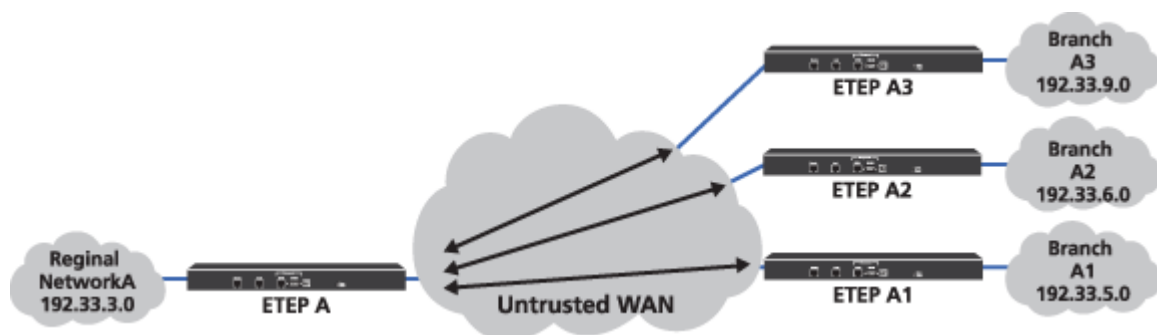
Table 55 Encrypt all mesh policy

Field	Setting
Name	Encrypt All Mesh
Priority	1000
Renew Keys/Refresh Lifetime	4 hours
Type	IPSec
IPSec	Encryption Algorithms - AES Authentication Algorithms - HMAC-SHA-1
Key Generation	By Network Set
Addressing Mode Override	Preserve internal network addresses
Minimize Policy Size	Disable
Network Sets	Network Set A Network Set B Network Set C Network Set D
Protocol	Any

Encrypt Traffic Between Regional Centers and Branches

In order to encrypt traffic between each regional center and its branches, four hub and spoke policies are required. The following figure illustrates the hub and spoke policy between Regional Network A and its branches: Branch A1, Branch A2, and Branch A3.

Figure 86 Regional center to branches hub and spoke policy



These hub and spoke policies require the four network sets created in [“Encrypt Traffic Between Regional Centers” on page 214](#) and twelve network sets for the branch networks.

Table 56 Network sets for the hub and spoke policies

	Networks	PEPs	Default ETKMS
Network Set A1	192.33.5.0 netmask 255.255.255.0	PEP A1	ETKMS 1
Network Set A2	192.33.6.0 netmask 255.255.255.0	PEP A2	ETKMS 1
Network Set A3	192.33.9.0 netmask 255.255.255.0	PEP A3	ETKMS 1
Network Set B1	172.44.5.0 netmask 255.255.255.0	PEP B1	ETKMS 1
Network Set B2	172.44.6.0 netmask 255.255.255.0	PEP B2	ETKMS 1
Network Set B3	172.44.7.0 netmask 255.255.255.0	PEP B3	ETKMS 1
Network Set C1	100.22.5.0 netmask 255.255.255.0	PEP C1	ETKMS 1
Network Set C2	100.22.7.0 netmask 255.255.255.0	PEP C2	ETKMS 1
Network Set C3	100.22.9.0 netmask 255.255.255.0	PEP C3	ETKMS 1
Network Set D1	100.33.2.0 netmask 255.255.255.0	PEP D1	ETKMS 1
Network Set D2	100.33.3.0 netmask 255.255.255.0	PEP D2	ETKMS 1
Network Set D3	100.33.5.0 netmask 255.255.255.0	PEP D3	ETKMS 1

The next three tables show the four regional hub and spoke policies.

Using Network Sets A, A1, A2, and A3, create a hub and spoke policy for region A as shown in the following table:

Table 57 Region A hub and spoke policy

Field	Setting
Name	Region A Hub and Spoke
Priority	900
Renew Keys/Refresh Lifetime	4 hours
Type	IPSec
IPSec	Encryption Algorithms - AES Authentication Algorithms - HMAC-SHA-1
Key Generation	By Network Set
Addressing Mode Override	Preserve internal network addresses
Minimize Policy Size	Disable
Hub	Network Set A
Spokes	Network Set A1 Network Set A2 Network Set A3
Protocol	Any

Using Network Sets B, B1, B2, and B3, create a hub and spoke policy for region B as shown in the following table:

Table 58 Region B hub and spoke policy

Field	Setting
Name	Region B Hub and Spoke
Priority	901
Renew Keys/Refresh Lifetime	4 hours
Type	IPSec
IPSec	Encryption Algorithms - AES Authentication Algorithms - HMAC-SHA-1
Key Generation	By Network Set
Addressing Mode Override	Preserve internal network addresses
Minimize Policy Size	Disable
Hub	Network Set B
Spokes	Network Set B1 Network Set B2 Network Set B3
Protocol	Any

Using Network Sets C, C1, C2, and C3, create a hub and spoke policy for region C as shown in the following table:

Table 59 Region C hub and spoke policy

Field	Setting
Name	Region C Hub and Spoke
Priority	902
Renew Keys/Refresh Lifetime	4 hours
Type	IPSec
IPSec	Encryption Algorithms - AES Authentication Algorithms - HMAC-SHA-1
Key Generation	By Network Set
Addressing Mode Override	Preserve internal network addresses
Minimize Policy Size	Disable
Hub	Network Set A
Spokes	Network Set A1 Network Set A2 Network Set A3
Protocol	Any

Using Network Sets D, D1, D2, and D3, create a hub and spoke policy for region D as shown in the following table:

Table 60 Region D hub and spoke policy

Field	Setting
Name	Region D Hub and Spoke.

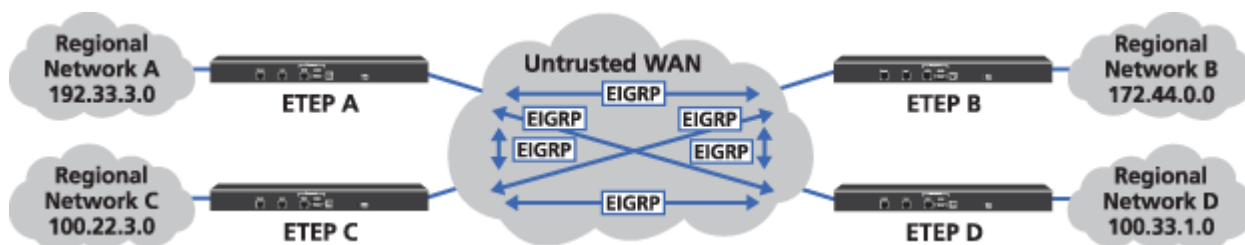
Table 60 Region D hub and spoke policy (continued)

Field	Setting
Priority	903
Renew Keys/Refresh Lifetime	4 hours
Type	IPSec
IPSec	Encryption Algorithms - AES Authentication Algorithms - HMAC-SHA-1
Key Generation	By Network Set
Addressing Mode Override	Preserve internal network addresses
Minimize Policy Size	Disable
Hub	Network Set D
Spokes	Network Set D1 Network Set D2 Network Set D3
Protocol	Any

Passing Routing Protocols

With Layer 3 routed networks, you might need to pass routing protocols in the clear. This is normally true when routers are placed behind the PEPs and when your WAN uses a private routed infrastructure. With a public routed infrastructure, the ISP handles the routing.

To create policies to pass routing protocols in the clear, include the router interfaces or subnets that participate in sharing the routing protocol. In our example, all the regional networks are Layer 3 routed networks and all branches are switched networks. Each regional network shares routing information with the other regional networks using EIGRP (protocol 88).

Figure 87 Passing routing protocol in the clear

Using the four network sets created in [“Encrypt Traffic Between Regional Centers”](#) on page 214, create a mesh policy as shown in the following table:

Table 61 Pass protocol 88 in the clear mesh policy

Field	Setting
Name	Clear EIGRP
Priority	2000 (higher priority than the Mesh encryption policy)
Renew Keys/Refresh Lifetime	4 hours
Type	Bypass
IPSec	
Key Generation	By Network Set

Table 61 Pass protocol 88 in the clear mesh policy (continued)

Field	Setting
Addressing Mode Override	Preserve internal network addresses
Minimize Policy Size	Disable
Network Sets	Network Set A Network Set B Network Set C Network Set D
Protocol	88

This policy must be set to a higher priority than the mesh policy created in [“Encrypt Traffic Between Regional Centers” on page 214](#). If this policy is set to a lower priority, the mesh encryption policy will override the bypass policy and the routing protocol will be encrypted.

Part IV Troubleshooting



17 ETEMS Troubleshooting

This section includes the following topics:

- [Possible Problems and Solutions](#)
- [Pinging the Management Port](#)
- [Retrieving Appliance Log Files](#)
- [Viewing Diagnostic Data](#)
- [Working with the Application Log](#)

Possible Problems and Solutions

The troubleshooting information in this section is grouped into categories. Within each category you will find a list of symptoms and possible solutions.


- [Appliance Unreachable](#)
- [Appliance Configuration](#)
- [Pushing Configurations](#)
- [Status Indicators](#)
- [Software Upgrades](#)

Appliance Unreachable



Symptom	Explanation and possible solutions
<p>Symptoms of ETEMS's inability to communicate with an appliance are:</p> <ul style="list-style-type: none"> • Status indicator of ?. • "Operation failed" result when putting a configuration to an appliance, refreshing status, or comparing configurations. • Unsuccessful software upgrade. 	<ul style="list-style-type: none"> • Check physical connectivity to the appliance's management port (proper seating of the RJ-45 Ethernet cable). • Verify that the management IP address is the same in ETEMS and on the appliance. Refresh the appliance status, and then compare configurations (Tools > Compare Config to Appliance). • The connection between ETEMS and the appliance has timed out. Check the timeout setting (Edit > Preferences) and adjust if necessary. • Check for a password mismatch between the appliance and ETEMS. Refresh the appliance status, and then look at the resulting error message or ETEMS log for a failure description. If the message indicates an invalid password, update ETEMS with the appliance password. • If IPSec is enabled on the management port, disable it and then disable the IPSec client. Verify that you can communicate with the appliance when IPSec is disabled. If not, check the preceding items to resolve the problem. If you can successfully establish communication with IPSec disabled, ensure that the IPSec client configuration matches the appliance's IPSec management port configuration. Enable IPSec on the management port and enable the IPSec client. If this does not fix the connectivity problem, see your system administrator or contact Customer Support.
<p>Unable to communicate with appliance via xml-rpc. Connection timed out.</p>	<p>Possible causes are:</p> <ul style="list-style-type: none"> • Appliance is unplugged or powered off. • Appliance is rebooting. • Communication timeout value is set too low (Edit > Preferences). • When managing ETEPs, TLS must be enabled in ETEMS. To check the TLS setting, go to Edit > Preferences > ETEMS > Communications and select Use TLS for XML/RPC. • When using trusted hosts on the ETEP, if you type the management station IP address incorrectly, EncrypTight will be unable to communicate with the ETEP. To recover, use SSh to log in to the CLI (Tools > Ssh). Log in as the ops or admin user, and at the command prompt type configure to enter configuration mode. From the <code>config></code> prompt, type disable-trusted-hosts to disable the trusted hosts entries for the ETEP.
<p>The appliance can communicate with the management station but is unable to respond to a request.</p> <p>The following error message may be displayed: <code>Appliance returned an unknown status code [-1]</code>.</p>	<ul style="list-style-type: none"> • Retry the operation. The appliance may have been in a transitional state and is now up and operational. • Connect to the appliance's CLI. Check for messages that provide an indication of the appliance's status. • Reboot the appliance from the CLI. After the appliance has rebooted, refresh the status. • If the above steps fail to clear the message, contact customer support.

Symptom	Explanation and possible solutions
<p>The ETEP cannot ping the management workstation.</p> <p>The request times out or returns an "Operation not permitted" message.</p>	<p>Check whether the trusted host feature is enabled on the ETEP.</p> <ul style="list-style-type: none"> Check the configuration for the trusted workstation. Pings are not allowed when the ICMP is unchecked in the trusted host configuration. You can disable trusted hosts from ETEMS or by issuing the disable-trusted-hosts CLI command.
<p>Cannot access the ETEP management port using SSH.</p>	<ul style="list-style-type: none"> Check the setting for the ssh-enable command. It must be set to true. Enabling FIPS mode or strong password enforcement on the ETEP causes the SSH daemon to restart, closing all open SSH connections. After enabling either of these features, wait 30-60 seconds before trying to re-establish an SSH connection to the ETEP management port. If you used SSH to manage the ETEP prior to replacing a certificate or entering FIPS mode, you may not be able to establish an SSH session after the configuration change. To correct this, clear the known host entry for your SSH client and retry.






Appliance Configuration

Symptom	Explanation and possible solutions
<p>Can't change the management port IP address on the appliance from ETEMS.</p>	<ul style="list-style-type: none"> The management port IP address must be unique. In the Appliances view, check for duplication. Verify that the appliance's management port is not in use by a CLI session or the appliance web interface.
<p>Editing the management IP address or date returns a  status.</p>	<ul style="list-style-type: none"> Refresh the appliance status. If the refreshed status is still not equal, compare the ETEMS and appliance configurations (Tools > Compare Config to Appliance) to determine which items are different. Make any necessary adjustments to synchronize the two configurations.
<p>Appliance setting is not displayed as a configuration option in ETEMS.</p>	<ul style="list-style-type: none"> Not all features are supported in each appliance model or software revision. Check the model number and software version configured for the appliance, then refer to the Factory Default tables in the configuration chapter for your appliance model to check feature availability.
<p>When configuring a new appliance, changing the product family (appliance model) causes other configuration settings to be discarded.</p>	<ul style="list-style-type: none"> To carry configurations forward when changing the product family, save the configuration prior to changing the product family.
<p>Can't change the appliance date or time from ETEMS.</p>	<ul style="list-style-type: none"> When the SNTP client is enabled on the appliance, you cannot change the appliance date or time. To modify the date or time, disable SNTP, push the configuration to the appliance, and then set the date (Edit > Date).

Pushing Configurations

Symptom	Explanation and possible solutions
New configuration isn't active on the appliance.	<ul style="list-style-type: none"> In the Appliances view, select the appliance and refresh its status. Some configuration changes require an appliance reboot to take effect. If the appliance status is , reboot the appliance (Tools > Reboot). If the ETEMS and appliance configurations are not equal, compare the configurations (Tools > Compare Config to Appliance) to determine the differences. Make any necessary adjustments to synchronize the two configurations.
After pushing a configuration to an appliance the ETEMS and appliance configurations are  .	<ul style="list-style-type: none"> Compare the configurations (Tools > Compare Config to Appliance) to determine the differences.
Can't push a configuration to an appliance.	<ul style="list-style-type: none"> Verify appliance reachability (see "Appliance Unreachable" on page 224).
Error communicating with the appliance. Read timed out.	<ul style="list-style-type: none"> The connection between ETEMS and the appliance has timed out. Check the communication timeout setting (Edit > Preferences) and increase if necessary.

Status Indicators

Symptom	Explanation and possible solutions
ETEMS and appliance configurations are not equal  .	<ul style="list-style-type: none"> Compare the ETEMS configuration to the appliance (Tools > Compare Config to Appliance). Do one of the following: 1) Copy appliance configuration settings to ETEMS or 2) Push the ETEMS configuration to the appliance.
Appliance requires a reboot  .	<ul style="list-style-type: none"> Some configuration changes require an appliance reboot to take effect (Tools > Reboot).
Policies need to be reloaded  .	<ul style="list-style-type: none"> The policies on the appliance have changed and require a reload to take effect (Tools > Reload Policies).
Appliance unmanageable  .	<ul style="list-style-type: none"> Check for a version incompatibility between the appliance model, software version, and EncrypTight. If you have a version incompatibility, delete the appliance configuration from ETEMS, then reenter it as a New Appliance with a supported configuration. See the <i>EncrypTight Release Notes</i> for a compatibility matrix. Check the ETEMS log (View > Application Log). If the log message indicates a runtime exception, contact Customer Support.
Status unknown ?	<ul style="list-style-type: none"> ETEMS has not yet queried the appliance status, or ETEMS is unable to communicate with the appliance (see "Appliance Unreachable" on page 224).
Appliance problem  .	<ul style="list-style-type: none"> The appliance is in an error state. See the user documentation for your appliance for troubleshooting information.

Software Upgrades

Symptom	Explanation and possible solutions
Can't download files from an FTP server.	<ul style="list-style-type: none"> Verify that the FTP server software is active on the specified host. Check the FTP server host, path, user ID, and password. Make sure that the following invalid characters are not used in the user ID and password: @ : ? # < > & Ping the FTP server and the appliance management port. If not successful, contact your Network Administrator.
Cannot communicate with an SFTP server.	<ul style="list-style-type: none"> Review the steps listed in the row above (FTP server verification). If you receive an error indicating that the ETEP cannot communicate with the SFTP server, log in to the CLI and issue the clear-known-hosts command. This will clear the existing known_host entries and allow you to re-enter the SFTP server IP address.
ETEMS cannot communicate with the appliance.	<ul style="list-style-type: none"> Verify appliance reachability (see "Appliance Unreachable" on page 224).
Can't determine status of ETEP software upgrade from ETEMS	<ul style="list-style-type: none"> ETEP upgrade status is reported in the system log at priority level "notice." System log messages that are sent to a syslog server can be used to monitor upgrade progress. From the console, two commands provide information about upgrades: show system-log and show upgrade-status.

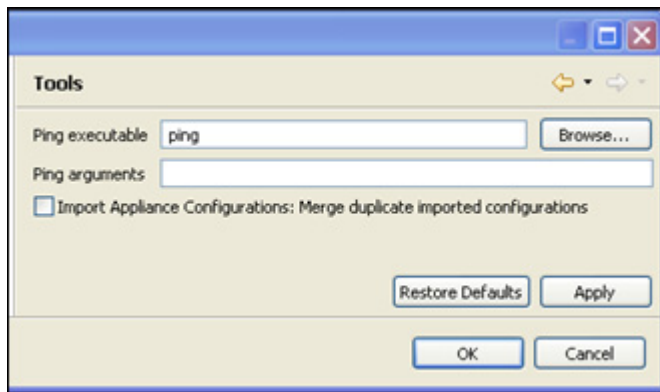
Pinging the Management Port

If ETEMS is having trouble communicating with an appliance's management port, try pinging the port to determine if the port is reachable from the management workstation.

To ping the management port:

- 1 In the Appliance Manager, select an appliance in the Appliances view.
- 2 In the Tools menu, click **Ping**. The ping command runs in a separate command window, where the results of the ping command are displayed.

You can override the operating system's default ping tool by specifying an alternative in the Preferences window.

Figure 88 Tools preferences**To change the default ping tool:**

- 1 In the Edit menu, click **Preferences**.
- 2 Click **ETEMS** to expand the tree, and then click **Tools** (Figure 88).
- 3 In the Tools window, browse to the location of the ping executable that you want to use.
- 4 *Optional*. Enter arguments to use with the ping command.
- 5 Click **Apply**, and then click **OK**.

Retrieving Appliance Log Files

You can retrieve and view log files from any appliance managed by ETEMS. Upon receiving a command from ETEMS, the selected appliances send their log files to the FTP server on the management workstation.

When retrieving log files from ETEP 1.6 and later appliances, you have the option of using FTP or SFTP for secure file transfer. If you choose SFTP as the connection method, all of the selected appliances must support SFTP.

When retrieving appliance log files, ETEMS combines all the log files from an appliance into a single file. It creates a directory named `cvLogFiles` in the FTP root directory, where the combined log files are stored as `.txt` files. The combined log file name is based on the appliance's management IP address and the timestamp of when the log was received. The filename format is:

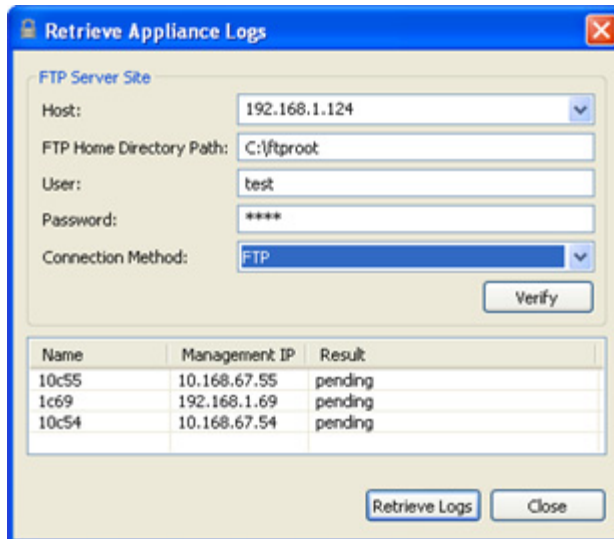
```
IPaddress_year_month_day_hour_minutes_seconds.txt.
```

The ETEP maintains log files per log facility in addition to the combined file. The individual log files are stored in `cvLogFiles\<managementIP>` in the FTP root directory. The subdirectory name, `<managementIP>`, is the ETEP's management IP address. Log file names are based on the log facility, such as `audit.log`, `snmp.log`, and `pki.log`. The log files have a `.log` extension and can be opened with any text editor. Archived log files have a `.gz` extension and can be decompressed with `gzip`, `WinZip`, or `7-zip`. Unlike the concatenated file, the log facility log files are overwritten each time log files are extracted from the appliance. To preserve a particular log file, rename it or move it to a different folder.

Log files are stored in the `cvLogFiles` directory until you manually delete them. When EncrypTight is uninstalled, the log files are not deleted.

To retrieve log files from an appliance:

- 1 Verify that an FTP server is running on the ETEMS workstation.
- 2 In the Appliance Manager, select the target appliances in the Appliances view. ETEMS can retrieve logs from multiple appliance in a single operation.
- 3 On the **Tools** menu, click **Retrieve Appliance Logs**.



- 4 In the Retrieve Appliance Logs window, enter the FTP server site information as described in [Table 62](#). Do not use the following special characters in the FTP user name and password: @ : ? # < > &.
- 5 Click **Verify** to confirm that the FTP site is valid. If it is not, ETEMS displays a message indicating the nature of the problem.
- 6 Click **Retrieve Logs**. The status of the operation is displayed in the Result column of the Retrieve Appliance Logs window.
- 7 When retrieving log files from a single appliance, ETEMS displays the log files in whatever application you have associated with .txt files, such as Notepad or WordPad. Log files are easier to read in WordPad than Notepad because of the line breaks that WordPad inserts in the file. When retrieving log files from multiple appliances, ETEMS does not automatically launch a log viewer application. Instead, select the log files of interest and open them with a text file editor.

Table 62 FTP server site information for log retrieval

Field	Description
Host	IP address of the management workstation. If you are retrieving log files from a host that has already been configured, you can select its IP address from the Host box. ETEMS completes the remaining FTP server information for you based on the selected host IP address. ETEP 1.6 and later appliances support IPv4 and IPv6 addresses. If you are using an IPv6 host address, all of the selected appliances must support IPv6.
FTP Home Directory Path	The path of the FTP root directory on the management workstation. You must enter the complete path. No other directories are allowed. ETEMS uses this path to locate the log files after they are uploaded from the appliance in order to display them.
User	User ID of a user on the FTP server. Do not use the following characters: @ : ? # < > &

Table 62 FTP server site information for log retrieval

Field	Description
Password	Password associated with the user name. Do not use the following characters: @ : ? # < > &
Connection Method	FTP is the default file transfer protocol and is supported on all appliance models and software revisions. SFTP provides secure file transfer. It is supported on ETEP appliances running version 1.6 and later software.

Viewing Diagnostic Data

ETEMS retrieves the following performance and diagnostic data from an appliance:

- Encryption statistics and a collection of frame and packet counters are displayed in the Statistics View.
- Local and remote port status and discarded packet information is displayed in the Status view.
- Security association database (SAD) and security policy database (SPD) information can be exported from the Statistics view to CSV files (ETEP only).

You can open Statistics or Status views for several appliances simultaneously. This can facilitate side-by-side comparisons of inbound and outbound traffic between appliances.



NOTE

Performance data varies among appliance models and software versions. If the statistics or status feature is not supported for your appliance, the menu item is grayed out.

Related topics:

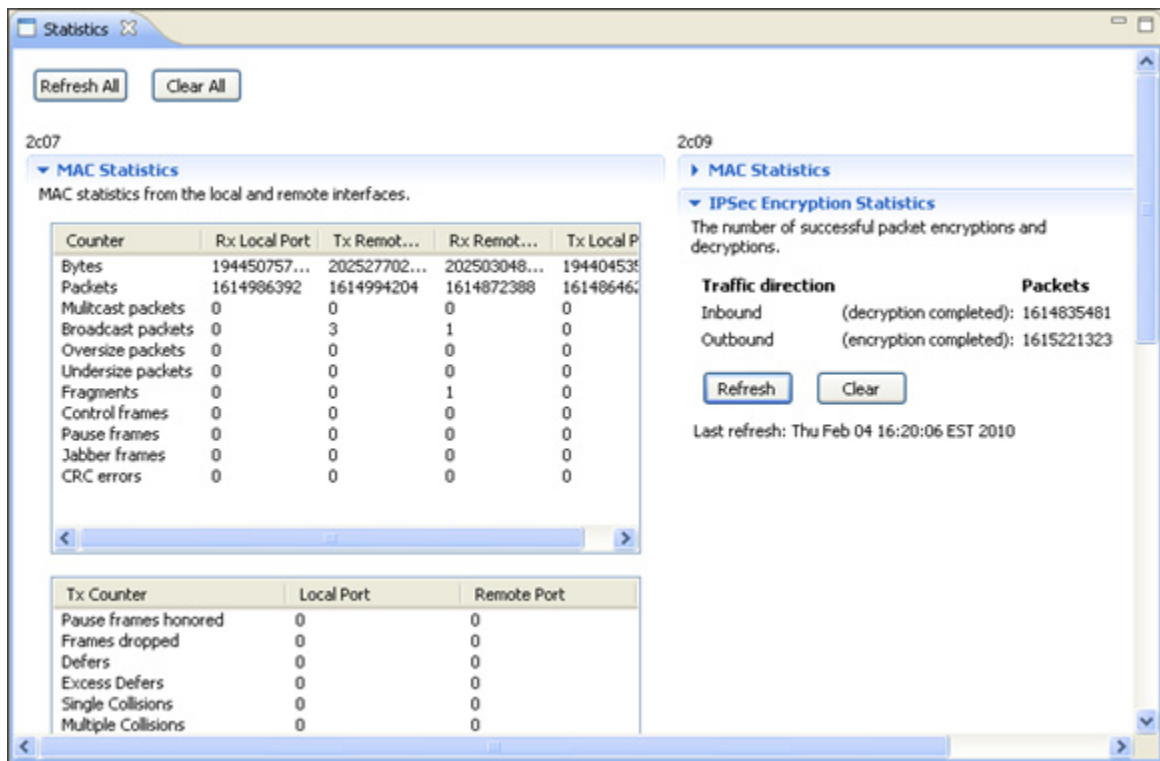
- [“Viewing Statistics” on page 230](#)
- [“Viewing Port and Discard Status” on page 232](#)
- [“Exporting SAD and SPD Files” on page 232](#)
- [“CLI Diagnostic Commands” on page 233](#)

Viewing Statistics

Statistics can assist with diagnosing and troubleshooting unexpected behavior of an EncryptTight appliance, and with performance monitoring. ETEMS displays a snapshot of the statistics when they are retrieved. Statistics vary by appliance model. See the user manuals for your appliance for more information.

ETEMS can display statistics for a single appliance or you can shift-click to select a group of appliances. When selecting a group of appliances, ETEMS displays the statistics for each appliance side-by-side. Use the horizontal scroll bar to view all of the selected appliances.

ETEMS retrieves statistics for up to 10 appliances at a time. If you select a larger number of appliances, ETEMS retrieves statistics from the next set of appliances as it completes the first group of 10. This continues until statistics have been retrieved for all of the selected appliances.

Figure 89 Encryption statistics and packet counters displayed for two ETEPs**To display statistics:**

- 1 In the Appliance Manager, select the target appliances in the Appliances view.
- 2 On the **View** menu, click **Statistics**. See [Table 63](#) for a description of ETEP statistics.
- 3 Click the **Refresh** or **Clear** button for the area of interest (IPSec Encryption Statistics or MAC/MIB2 Statistics). Each area has its own independent clear and refresh functions. When viewing statistics for a group of appliances, the Refresh All and Clear All buttons at the top of the view act on all of the selected appliances.

The **Refresh** button updates the counters display. The behavior of the Clear button varies by appliance model. On the ETEP, the **Clear** button resets the counters on the appliance *and* in ETEMS.

Table 63 ETEP Statistics

Statistic	Description
Encryption statistics	The number of packets successfully encrypted and decrypted.
MAC statistics	Displays a variety of frame and packet counts on the local and remote interfaces: <ul style="list-style-type: none"> • Transmit counters on the local and remote ports • Receive counters on the local and remote ports • Combined transmit and receive counters by frame size • Other counters sent and received on the local and remote ports
Clear button	Resets the counters display to zero and resets the counters on the ETEP. The Statistics window has two clear buttons: one controls the encryption statistics and the other controls the MAC statistics.

Viewing Port and Discard Status

The Status view displays information about local and remote port status, and discarded packets. Port status is available only for ETEPs. The details displayed for discarded packets varies by appliance model. See the user manuals for your appliance for more information.

Figure 90 ETEP port status and discarded packets counts

	Local Interface	Remote Interface
Operational status:	up	down
Physical address:	0:9:ed:0:18:e1	0:9:ed:0:18:e0
Speed:	10 MBit	10 MBit
MTU:	1500	1500

Discard Reason	Total Dropped
Fragmentation error	0
ICMP non-zero fragment	0
Reassembly error	0
Internal packet order error	0
Internal packet queue error	0
Management port forwarding error	0
Management port packet RX error	490
Remote port packet RX error	0
Local port packet RX error	0
Linux ngt ready error	0

To display status:

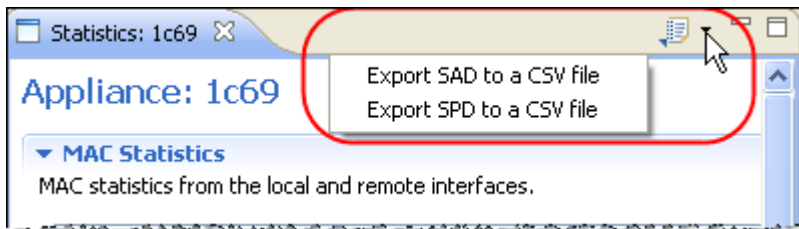
- 1 In the Appliance Manager, select the target appliance in the Appliances view.
- 2 On the **View** menu, click **Status**.
- 3 Click **Refresh** or **Clear**. The **Refresh** button updates the discard counters. The behavior of the **Clear** button varies by appliance model. On the ETEP, the **Clear** button resets the discard counters on the appliance *and* in ETEMS.

Exporting SAD and SPD Files

Security policies are rules that tell an encryption appliance how to process different packets that it receives. Security policies are stored in the appliance's security policy database (SPD).

A security association (SA) is a set of information that describes the particular security mechanisms that are used for secure communications between two appliances. The appliance's security associations are contained in its security association database (SAD).

ETEMS can export the SPD and SAD from the ETEP to a CSV file to aid in policy troubleshooting. See the *ETEP Installation Guide* for more information about the information contained in the SPD and SAD.

Figure 91 Export the SAD or SPD to a CSV file**To export the SAD or SPD from the ETEP:**

- 1 In the Appliance Manager, select the target appliance in the Appliances view.
- 2 On the **View** menu, click **Statistics**.
- 3 In the upper right corner of the Statistics view, click the Export menu button. From the list, choose which file to export (SAD or SPD).
- 4 You will be prompted to save the CSV file. Browse to a location on the hard drive and click **Save**.
- 5 To open the CSV file in an editor, click **Yes** when prompted. Windows opens the file with whatever application you have mapped to the .csv file extension. Click **No** to complete the export operation without viewing the file.

Figure 92 SPD exported to an Excel spreadsheet

Ethernet Type	VLAN ID	Direction	Policy Type	Priority Index	IP Protocol	Destination IP	Destination IP Subnet M	Destination P
2048	"any"	"Inbound"	"None"	"2147483647"	"6"	"0.0.0.0"	"0.0.0.0"	"any"
2048	"any"	"Outbound"	"None"	"2147483647"	"6"	"0.0.0.0"	"0.0.0.0"	"any"
2048	"any"	"Inbound"	"None"	"2147483646"	"6"	"0.0.0.0"	"0.0.0.0"	"443"
2048	"any"	"Outbound"	"None"	"2147483646"	"6"	"0.0.0.0"	"0.0.0.0"	"443"

CLI Diagnostic Commands

You can access the appliance CLI from ETEMS to perform appliance level troubleshooting.

Show commands are useful for diagnostics. Using various **show** commands you can view the appliance configuration and IPsec diagnostics such as discarded packets, encryptions statistics, and active security associations. See your appliance's user manuals for more information about CLI commands.

To access the appliance CLI:

- 1 Make sure that you can connect using the client available for your appliance model. ETEP appliances use SSH to connect to the appliance. No configuration is required for SSH.
- 2 In the Appliance Manager, select the target appliance in the Appliances view.
- 3 On the **Tools** menu, click **SSH** to connect to the appliance's CLI.
- 4 Enter the user name and password to log in to the CLI as **ops** or **admin**. Once you are logged in, you can issue all CLI commands available to your user type.
- 5 To terminate the session, log out of the CLI and return to the EncrypTight application.

Working with the Application Log

The application log provides information about significant events and failures with EncrypTight. The application log captures events specific to ETEMS and ETPM and their interaction with appliances. The user ID associated with an event is recorded in the log.

The following types of events are recorded in the EncrypTight application log:

- Successful and failed attempts to log in to the EncrypTight application
- Communication attempts with the appliance: pushing configurations, status refreshes, reboot requests, software upgrades, FTP file transfers
- Appliance additions or deletions from ETEMS
- Changes to ETEMS Preferences
- Telnet, SSH, or web interface connections to an appliance
- Communication failures between ETEMS and the appliance (unable to log in, connection timed out, connection refused). See [“Possible Problems and Solutions” on page 223](#) for suggested solutions to these problems.
- Runtime exceptions, which occur when incorrect or corrupted data is sent by ETEMS, ETPM, or the appliance. Contact customer support if you receive an error of this type.

EncrypTight provides several options for viewing application log events. You can view log events from within EncrypTight, configure EncrypTight to send log events to a syslog server, or export the log as a text file.

The EncrypTight application log is different from the appliance log, which captures events about the operation of a particular appliance. To learn how to retrieve and view appliance logs, see [“Retrieving Appliance Log Files” on page 228](#).

Related topics:


- [“Viewing the Application Log from within EncrypTight” on page 234](#)
- [“Sending Application Log Events to a Syslog Server” on page 235](#)
- [“Exporting the Application Log” on page 235](#)
- [“Setting Log Filters” on page 235](#)
- [“Other Application Log Actions” on page 236](#)
- [“ETPM Log Files” on page 241](#)

Viewing the Application Log from within EncrypTight

You can view the log information on the screen to review recent application events and activity. You can view the application log from ETEMS and ETPM.

To view the log information:

- 1 From either ETEMS or ETPM, click **View > Application Log**. The Log view opens to display the most recent entries in the log. To view more detailed information about a specific entry, double-click the entry.
- 2 To display the application log view in the foreground whenever a new event is written to the log, do the following:

- a On the application log tool bar, click .
- b In the application log menu, click **Activate on new events**. A check mark appears next to this menu item when the feature is active. Click the menu item to toggle the feature on and off.

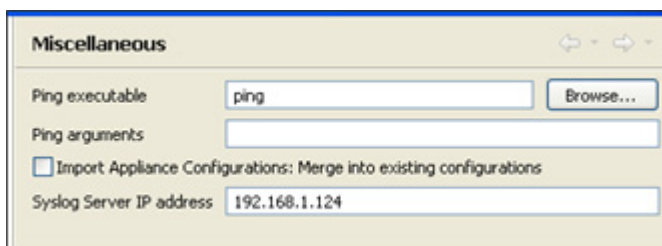
Sending Application Log Events to a Syslog Server

EncryptTight can send application log events to a syslog server.

To configure a syslog server:

- 1 In the ETEMS Appliance Manager, click **Edit > Preferences**.
- 2 Click **ETEMS** to expand the tree, and then click **Miscellaneous**.
- 3 In the Miscellaneous window, enter the IP address of the syslog server. The syslog server address can be in IPv4 or IPv6 format.
- 4 Click **Apply**, and then click **OK**.

Figure 93 Syslog server preference



Exporting the Application Log

Exporting the application log saves the log to a text file.

To export the log file:

- 1 In the Log view, click the **Export Log** button.
- 2 Name the log file and save it. The log is a text file with a `.log` extension.

Setting Log Filters

Log filters control the kind of information that appears in the application log file:

- Type of events
- Number of events that are visible
- Whether the information persists across sessions

To change the application log filters:


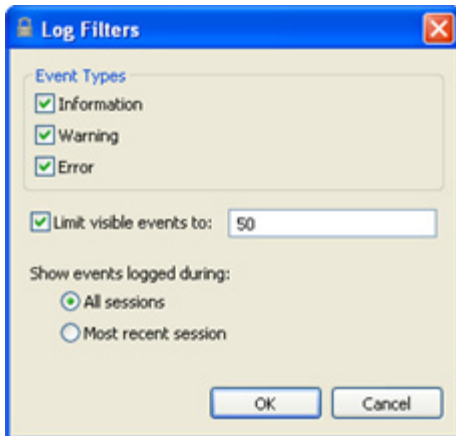
- 1 On the application log tool bar, click .
- 2 In the application log menu, click **Filters**.
- 3 Set the log filter criteria, and then click **OK**.

Figure 94 Application log filters










 **NOTE**

Increasing the visible event limit to a large number (more than 200) can noticeably slow the speed at which EEMS updates appliance status. If you notice that status refreshes are abnormally slow, clear application log file and reset the visible events limit to a lower value.

Other Application Log Actions

You can perform the following actions from the Log view using the buttons shown in [Table 64](#).

Table 64 Log File Actions

Icon	Description
	Exports a log file from the Log viewer to another location on the hard drive.
	Imports a log file from a specified location into the Log viewer. The imported file is read-only; new events are not written to the imported file.
	Clears the entries displayed in the Log viewer.
	Deletes the log file.
	Opens the log file in a text editor. This makes it easier to view a long list of entries.
	Restores recently cleared log entries.
	Opens the application log menu.

18 ETPM and ETKMS Troubleshooting

This section provides information to help you with ETPM and ETKMS problem resolution, including:

- [Learning About Problems](#)
- [ETKMS Troubleshooting Tools](#)
- [PEP Troubleshooting Tools](#)
- [Troubleshooting Policies](#)
- [Solving Network Connectivity Problems](#)
- [Modifying EncrypTight Timing Parameters](#)
- [Certificate Implementation Errors](#)

Learning About Problems

Troubleshooting the EncrypTight system should start with the status monitoring feature on the Policy Manager (ETPM). Log files in ETPM, on the ETKMS, and on the PEPs can further aid support and IT personnel in locating problem areas.

External ETKMSs and the PEPs include other troubleshooting aids. For complete information about troubleshooting PEPs, see the documentation for the PEPs that you use.








This section includes the following topics:

- [“Monitoring Status” on page 237](#)
- [“Symptoms and Solutions” on page 238](#)
- [“Viewing Log Files” on page 241](#)


Monitoring Status

As soon as you deploy the policies, the ETPM status indicators change to yellow momentarily. When the policies are successfully deployed, the status indicators change to green. The status indicator shown next to the policy name reflects the overall status of all the components that constitute the policy. To see the status of the individual components, expand the policy tree. [Table 65](#) lists each of the possible status indicators.

Table 65 ETPM status problems and solutions

Indicator	Explanation and Possible Solutions
Status Unknown 	<p>The current status is unknown or questionable. This state can occur if:</p> <ul style="list-style-type: none"> A policy or a component of a policy has been changed and the policy has not been deployed. In this case, the indicator appears next to only those policies where changes have been made to the policy or its components. Deploy the policies. The application was closed and then restarted. In this case, the indicator appears next to all policies. Refresh the status of the policies and their components. If the status does not return to a green indicator, redeploy the policies.
Pending 	ETPM performed an action and is waiting for responses from the ETKMSs.
Consistent 	ETPM performed an action and the responses from the ETKMSs indicate that the PEPs are consistent with the settings in ETPM.
Inconsistent 	<p>Deployed policies in a PEP do not match the policies in ETPM or no policy is present.</p> <ul style="list-style-type: none"> Check the Policy view to locate which PEP has the inconsistency and redeploy policies
Communication error 	<p>A communication error or timeout has occurred with one or more PEPs included in the policy.</p> <ul style="list-style-type: none"> Expand the policy view to locate which PEPs have the error. Check the ETPM application log to find more detailed information on the error. If the error occurred on the ETKMS or PEP, check those logs for additional information. Check the communication links from ETPM to ETKMS and ETKMS to PEP. If the trusted host feature is enabled on a PEP, you must push the configuration to the PEP to add the ETKMS to the PEP's trusted host list. To resolve the communication error, push the appliance configurations to the PEPs and then redeploy the policy.
Configuration error 	<p>A configuration error has been detected in one of the policy components.</p> <ul style="list-style-type: none"> Expand the policy to find the configuration error indicator in one of the policy components. Double-click the component to view the editor and find the entry with the configuration error. You can mouse over the  in the editor to view a message describing the error.


**TIP**

After you deploy policies, if the indicators are anything other than green, click **Refresh Status**  before you take other troubleshooting actions.

Symptoms and Solutions

This section discusses some symptoms that you might encounter while using ETPM. For some of these symptoms, you might want to check the log files to gather more information. For information about working with log files, see [“Viewing Log Files” on page 241](#).




 **NOTE**

Always check the status of the PEPs in the Policy View after deploying policies, refreshing status, or renewing keys. All PEPs should show a Consistent indicator .





This section includes the following topics:

- “Policy Errors” on page 239
- “Status Errors” on page 240
- “Renew Key Errors” on page 240


Policy Errors

Symptom	Explanation and possible solutions
Policies are not executing as expected.	<p>Check the policy priorities for uniqueness. Do not give multiple policies the same priority.</p> <p>Check the policy priorities to make sure the relative ordering is correct. Policies are executed from highest to lowest priority.</p>
Policy and network configuration in ETPM is not saved.	Data is not saved until you add at least one PEP in ETEMS. Follow the workflow outlined in the <i>EncryptTight User Guide</i> .
A policy deployment operation times out and the policies are marked with the yellow Pending indicator  . If you then refresh status, all policies will be marked with the red Inconsistent indicator  .	<p>If you attempt to deploy a policy file to ETEP PEPs that is larger than the maximum size for the model, the ETEP PEP generates an error and rejects the policy file. The error is recorded in the ETKMS log file. However, ETPM does not detect the error.</p> <p>As a workaround, reduce the number of network sets or networks used in the policy and try to redeploy until all of the policies are marked with a green Consistent indicator. For more information about policies and the operational limits of ETEP PEPs, see the <i>EncryptTight User Guide</i>.</p>
<p>Policy deployment fails and ETPM displays the following message:</p> <pre>Failed to complete Deployment The deployment operation failed on a ETKMS - connection timed out: ETKMS <ETKMS IP Address></pre>	<p>This message appears when the ETKMS with the specified IP address cannot be reached. If you have a primary and a backup ETKMS, this error does not indicate that the overall policy deployment failed. If the failure is with the primary ETKMS, the backup ETKMS takes over policy and key deployment to the PEPs. If the failure is with the backup ETKMS, the primary ETKMS continues to deploy policies and keys to the PEPs.</p> <p>Check the status indicator in the Policy view of the ETPM for all PEPs. If the status shows a  indicator, the PEPs received the appropriate policies and keys; otherwise, the PEPs did not receive the policies and keys and immediate action is required to prevent network outages.</p>

Status Errors

Symptom	Explanation and possible solutions
ETEMS cannot verify that the software version installed on the ETKMS matches the version selected in the Appliance Manager.	In the Appliance Manager in ETEMS, when you refresh status for a ETKMS, the ETKMS does not return information regarding the version of the ETKMS software that is running on the ETKMS. Log in directly to the ETKMS or use an SSH client to log in remotely, and type the following command: rpm -qi etkms
Cannot refresh the status of a new ETKMS in ETEMS.	Deploy policies from ETPM, and then refresh the status of the ETKMS.
ETPM reports that the policy deployment was successful, but all of the PEPs are marked with the  indicator and did not get the policy.	Make sure that you entered the correct name for the ETKMS in the ETEMS Appliance Manager. This error is recorded in the application log and in the kdist.log file on the ETKMS. A mismatch between the name displayed in the Appliance Manager and the actual name of the ETKMS can cause communication failures between the ETKMS and the PEPs.
After adding a PEP in the Appliance Manager and pushing the configuration to the PEP, the status shown in the PEP tab in ETPM is not correct and indicates a  .	After adding a new PEP in the Appliance Manager and viewing the incorrect PEP status in ETPM, switch to the Appliance Manager and then switch back to ETPM. The status indicator for the new PEP should be correct.
The Renew Keys operation does not indicate success or failure for backup ETKMSs.	Click Refresh Status in ETPM and verify that the backup ETKMS is providing coverage and reporting status.
If you add a PEP to an existing policy and do not immediately redeploy the policy, but later refresh the status or renew keys, the policy will be marked with the red exclamation mark  .	The  indicator is typically used to indicate communication errors. In this case the policy does not yet exist on the PEP and cannot be rekeyed or refreshed.

Renew Key Errors

Symptom	Explanation and possible solutions
The PEP CLI is unavailable during a deployment or rekey.	Large policy deployments or rekeys can prevent access to the command line interface (CLI) of a PEP while the PEP is processing the current operation. Automatic network management system polling during this period can result in an incorrect report that the PEP is out of service. Wait a few minutes for the current operation to complete, and then retry.
A Renew Keys operation fails for a specific ETKMS and ETPM displays the following message: Renew keys operation status The Renew keys operation failed for the following ETKMSs <list of ETKMS IP addresses that failed>	This message appears when the ETKMSs listed in the error message could not be reached during a Renew Keys operation. The Renew keys operation was successful for all other ETKMSs. To ensure that all PEPs received policies and keys, check the status indicator in the Policy View of the ETPM for all PEPs. If the status shows a  indicator, the PEPs received the appropriate keys; otherwise, the PEPs may not have received one or more keys and immediate action is required to prevent network interruption.

Viewing Log Files

Each component in the EncrypTight system creates and maintains log files that you can use to troubleshoot issues. This section includes the following topics:

- [“ETPM Log Files” on page 241](#)
- [“ETKMS Log Files” on page 241](#)
- [“PEP Log Files” on page 242](#)

ETPM Log Files

ETPM and ETEMS record significant events and failures in the application log. The application log file is a fixed length list of entries that records significant events and failures in ETEMS and ETPM.

The events recorded in the application log include:

- Communication operations and failures
- SSH connections
- Runtime exceptions, which occur when incorrect or corrupted data is sent by ETEMS or ETPM, or received from a PEP. Contact customer support if you receive an error of this type.

EncrypTight provides several options for viewing application log events. You can view log events from within ETPM or ETEMS by selecting **View > Application Log** on the main menu bar. You can also configure EncrypTight to send log events to a syslog server, or export the log as a text file.

For more information on the application log, refer to [“Working with the Application Log” on page 234](#).

ETKMS Log Files

Each ETKMS creates a daily log file (kdist.log) and stores these files in the /var/log/etkms directory on an external ETKMS and in the \tools\ETKMS\log directory on a local ETKMS (relative to the installation directory). These logs provide information about significant events and failures in ETKMS communications with the ETPM and PEPs. View the daily log file with any text editor for each day in question. Communications failures are clearly marked with an ERROR tag.

When the ETKMS saves a daily log file in order to start a new one, it names the file as

```
kdist.log.xxxx-xx-xx
```

where `xxxx-xx-xx` is the year, month and date of the log file (for example, 2010-05-05).

You can view the available log files with a text editor. With external ETKMSs, you need to log in directly on the ETKMS server (if you have physical access to the ETKMS), or you can use an ssh client to log in remotely and retrieve the log file.

On a periodic basis, you can delete or archive any or all of these daily log files without affecting the operation of the ETKMS or EncrypTight.

PEP Log Files

You can retrieve and view log files from any PEP using ETEMS. When a PEP receives a command from ETEMS, it sends its log files to the designated FTP server. To use this feature you must have FTP server software running on the ETEMS workstation.

If a PEP contains several log files, ETEMS combines the log files into a single file. ETEMS creates a directory named cvLogFiles in the FTP root directory, where the combined log files are stored as .txt files. The combined log file name is based on the appliance's management IP address and the timestamp of when the log was received.

For more information about working with log files, refer to [“Retrieving Appliance Log Files” on page 228](#).

The available logging configuration settings vary depending on the model of the PEP. For more information, refer to the configuration chapter for your PEP.

ETKMS Troubleshooting Tools

External ETKMSs provide a number of tools that you can use to troubleshoot problems.

This section includes the following topics:

- [“ETKMS Server Operation” on page 242](#)
- [“Optimizing Time Synchronization” on page 243](#)
- [“Shutting Down or Restarting an External ETKMS” on page 243](#)
- [“Resetting the Admin Password” on page 243](#)

ETKMS Server Operation

This section describes some Linux commands that are useful for identifying the applications and services running on an external ETKMS. If you have physical access to the ETKMS, you can log in directly on the ETKMS server, or you can use an ssh client to log in remotely.

Table 66 Linux Commands

Command	Description
<code>chkconfig --list</code>	Lists the configuration status of each known application that started at each of the various run levels.
<code>chkconfig --list fgrep "3:on"</code>	Lists the configuration status of applications that started at run level 3. This is the normal operating level for the Linux operating system.
<code>service --status-all</code>	Lists the status of all known services.
<code>service --status-all fgrep "is running"</code>	Lists the status of services that are currently running.

Optimizing Time Synchronization

With NTP, time synchronization does not always happen instantaneously. If the time difference between the ETKMS (or any system component) and the NTP server is large enough, it can take a significant amount of time to synchronize. If this occurs, you can use the following command to set up *step-ticker* files that can improve the performance of the NTP service.

To optimize the NTP service:

- 1 Log into the ETKMS and type, all on one line:

```
awk '/^server/ {print $2}' /etc/ntp.conf | grep -v '127.127.1.0' > /etc/ntp/step-tickers
```

And press **Enter**.

Shutting Down or Restarting an External ETKMS

If necessary, you can restart the ETKMS server or shut down the ETKMS server completely. If you need to relocate the ETKMS server, shut it down first.

To shut down or restart the ETKMS server:

- 1 Log in as root.
- 2 Do one of the following:
 - To reboot immediately, type **reboot**.
 - To shut down the ETKMS server completely, type **shutdown -h now**.

For information about starting and stopping a local ETKMS, see [“Basic Configuration for Local ETKMSs” on page 44](#).

Resetting the Admin Password

If you lose or forget the password to the admin account, you will not be able to log into an external ETKMS remotely. You can log in as root and change the password for the admin account, but the root user cannot log in remotely. To reset the admin password, you need to access the ETKMS directly and log in as root.

PEP Troubleshooting Tools

This section includes the following topics:

- [“Statistics” on page 244](#)
- [“Changing the Date and Time” on page 244](#)
- [“ETEP PEP Policy and Key Information” on page 244](#)
- [“Replacing Licensed ETEPs” on page 245](#)

Statistics

For ETEP PEPs, you can use the Statistics view in the ETEMS Appliance Manager to display encryption statistics and packet counters. This includes information about packet encryptions and decryptions. The exact statistics displayed vary depending on the model of the PEP that you select. You can also use the Status view to see information about discards.

To view statistics:

- 1 In the Appliance Manager perspective, select the target PEP.
- 2 Click **View > Statistics** or **View > Status**.

Changing the Date and Time

Ordinarily, all EncryptTight components should be synchronized with an NTP server. However, if an NTP server becomes unavailable or unreachable for a significant length of time, the time on your PEPs can drift out of sync significantly. The best option in this situation is to select a different, reachable NTP server.

If this is not possible, you can temporarily disable the SNTP client on the PEPs and change the time and date on the PEPs from the ETEMS Appliance Manager. You can change the time and date for a specific PEP or multiple PEPs. If the selected PEPs are ETEP PEPs or include a mix of appliance models, enter the date and time relative to UTC.



Because time synchronization with an NTP server is critical to the EncryptTight system, this procedure should only be used for troubleshooting purposes and only as a temporary fix. For complete information on using this feature, see [“Changing the Date and Time” on page 120](#). Note that you must disable the SNTP client first. This operation fails if the SNTP client is enabled.

To disable the SNTP client on multiple PEPs:

- 1 Select the PEPs that you want to change.
- 2 Select **Edit > Multiple Configurations > SNTP Client**.
- 3 Clear the **Enable** checkbox.
- 4 Click **Apply**.
- 5 Push the new configuration to the PEPs.

To change the date and time on multiple PEPs:

- 1 Select the PEPs that you want to change.
- 2 Select **Edit > Date**.
- 3 Enter the date and time in the appropriate boxes.
- 4 Click **Apply**.

ETEP PEP Policy and Key Information

In addition to exporting various logs from ETEP PEPs, you can export the Security Policy Database (SPD) and the Security Association Database (SAD). The SPD stores information on each policy

deployed to the PEP, including the destination and source IP addresses, priority, and the policy type. The SAD includes information on every security association (SA) established between the ETEP PEP and another appliance.

You can use this information to help you troubleshoot policy problems involving ETEP PEPs. You can use ETEMS to export the SPD and SAD to CSV files.

To export SAD or SPD files from ETEP PEPs:

- 1 In the Appliance Manager, select the target ETEP PEP in the Appliances view.
- 2 Click **View > Statistics**.
- 3 In the upper right corner of the Statistics view, click the **Export** button. From the list, choose which file to export (SAD or SPD).
- 4 You will be prompted to save the .csv file. Browse to a location on your hard drive and click **Save**.
- 5 To open the .csv file, click **Yes** when prompted. Windows opens the file with whatever application is associated with the .csv file extension. Click **No** to complete the operation and without viewing the file.



TIP

The .csv files can be easier to read and work with if you import them into a spreadsheet application such as Microsoft Excel.

Related topic:

- [“Exporting SAD and SPD Files” on page 232](#)

Replacing Licensed ETEPs

In the event that you need to replace an ETEP with software version 1.6 and later, you must generate and install a new license on the replacement before you can use it. For instructions on how to install licenses, see [“Managing Licenses” on page 56](#).

Troubleshooting Policies

Many problems with encryption and policies can be solved by changing the priorities assigned to the policies. If the policy priorities are not correctly assigned, traffic can be dropped or mistakenly sent in the clear. To troubleshoot these issues, first check to see if traffic is being passed or encrypted.

- [“Checking Traffic and Encryption Statistics” on page 245](#)
- [“Solving Policy Problems” on page 246](#)

Checking Traffic and Encryption Statistics

To check if traffic is being passed or encrypted using the Statistics view:

- 1 In the Appliances view, click the target PEP to select it.
- 2 Click **View > Statistics**.

- 3 In the MAC Statistics section (for ETEP PEPs), note the values in the Transmit and Receive packet entries for the Local and Remote interfaces (Local Port and Remote Port).
 - If packets are being received on the Local interface and transmitted on the Remote interface, traffic is being passed in the outbound direction. If packets are not being transmitted on the Remote interface, traffic is not being passed.
 - If packets are being received on the Remote interface and transmitted on the Local interface, traffic is passing in the inbound direction. If packets are not being transmitted on the Local interface, traffic is not being passed.
- 4 In the IPsec Encryption Statistics section of the Statistics view, note the values in Inbound and Outbound traffic directions.
 - If inbound traffic is being received, but the **Inbound (decryption completed)** count is zero, traffic is not being decrypted.
 - If outbound traffic is being transmitted, but the **Outbound (encryption completed)** count is zero, traffic is being sent in the clear.

With ETEP PEPs, you can only view decryption completed and encryption completed counts. You cannot view the decryption and encryption attempted counts. However, you can click **View > Status** to see discard counts.

Solving Policy Problems

If you have confirmed that the PEP is not encrypting traffic, the priority settings for your policies could be incorrect. Each PEP implements policies based on the priority and data filtering criteria set on each policy. You can also experience policy problems if you restore a previous file system on a PEP and inadvertently restore policies or certificates that have expired.

The following topics can help you identify and resolve policy problems:

- [“Viewing Policies on a PEP” on page 246](#)
- [“Placing PEPs in Bypass Mode” on page 246](#)
- [“Allowing Local Site Exceptions to Distributed Key Policies” on page 247](#)
- [“Expired Policies” on page 247](#)
- [“Cannot Add a Network Set to a Policy” on page 248](#)
- [“Packet Fragments are Discarded in Point-to-Point Port-based Policies” on page 248](#)

Viewing Policies on a PEP

For ETEP PEPs, export the SPD to view the policies that are in effect (for more information, see [“Exporting SAD and SPD Files” on page 232](#)).

Look at the priority and data filtering criteria for each policy implemented on the PEP. Look for clear policies at a higher priority than an encrypt policy for the same data that will override the encrypt policy. If you identify such a policy, change the priority of the policy in ETPM and redeploy your policies.

Placing PEPs in Bypass Mode

For troubleshooting policy problems, it can be helpful to place the PEPs in bypass mode to verify that traffic can pass in the clear.

Do one of the following:

- In the Appliance Manager view, select the ETEP and choose **Tools > Clear Policies**.
- In ETPM, create a bypass policy and deploy it to the PEPs.
- For distributed key policies: In ETEMS, change the Encryption Policy setting on the Features tab from Layer 2 to Layer 3 (or vice versa), and push the configuration to the ETEP. Encrypt and drop policies are removed from the ETEP, and traffic passes in the clear until you create and deploy new policies.
- For Layer 2 point-to-point policies: In ETEMS, change the Traffic Handling setting on the Policy tab to EthClear, and push the configuration to the ETEP.

Related Topics:

- [“Deleting Policies” on page 209](#)

Allowing Local Site Exceptions to Distributed Key Policies

Local site policies allow you to create locally configured policies using CLI commands, without requiring an ETKMS for key distribution. Using the local-site CLI commands you can create manual key encryption policies, bypass policies, and discard policies at either Layer 2 or Layer 3.

The primary use for local site policies is to facilitate in-line management in Layer 2 encrypted networks. These policies supplement existing encryption policies, adding the flexibility to encrypt or pass in the clear specific Layer 3 routing protocols, or Layer 2 Ethertypes and VLAN IDs.

The local-site policy feature gives you the ability to define a set of policies for the in-line management protocols that need to be passed through the ETEP, such as EIGRP, OSPF, RIPv2, or BGP. These policies are high priority policies that are not affected when EncrypTight distributed key policies are deployed on the ETEP.

This feature is similar to the ETEP configuration option that allows TLS traffic to pass through the ETEPs in the clear, but it provides the additional flexibility of allowing you to specify several protocols and ports, and to restrict the policy to specific IP addresses. The policy action can be defined as Clear, Drop or Protect. Protect policies allow the in-line management traffic to be encrypted with user-defined manual keys.

You can use the local-site CLI commands to create a variety of policies:

- Pass Layer 3 routing protocols in the clear when encrypting traffic at Layer 2
- Encrypt in-line management traffic that is typically passed in the clear when deploying EncrypTight policies, such as TLS and ARP packets
- Create manual key encryption policies for Layer 2 or Layer 3 traffic
- Create discard policies based on Layer 2 selectors (Ethertype or VLAN ID) or Layer 3 selectors

To learn how to create local site policies to supplement your EncrypTight distributed key policies, see the *ETEP CLI User Guide*.

Expired Policies

Whenever you restore a previous file system on a PEP, it is possible that you could also restore a set of expired policies, old certificates, and out of date keys inadvertently. This can cause a number of different policy-related problems and affect communications between the ETKMS and the PEP.

To fix these issues, redeploy your policies from ETPM to make sure that your PEPs have current policies and keys.

Cannot Add a Network Set to a Policy

Non-contiguous subnet masks are supported on ETEP PEPs version 1.4 and later. When you use non-contiguous network masks, the network set must include a PEP that supports the feature. In addition, all network sets in a policy must include supporting PEPs. ETPM prevents you from dragging non-supporting elements into a network set or policy when non-contiguous networks masks are in use.

Packet Fragments are Discarded in Point-to-Point Port-based Policies

Packet fragments are incorrectly discarded in point-to-point port-based policies when packets exceed the PMTU and are therefore fragmented and reassembled. This occurs only when the ETEP Encryption Policy Setting is configured as Layer 3:IP (ETEMS Features tab), and any of the following conditions are met:

- When the ETPM policy type is Bypass, the ETEP discards packet fragments in Layer 3 and Layer 4 policies.
- When the ETPM policy type is IPSec, the ETEP discards Layer 3 packet fragments.
- When the ETPM policy type is IPSec, the ETEP discards Layer 4 packet fragments when the Reassembly mode is set to Gateway.




Workarounds:

- Create a point-to-point policy that is not port-based. In the ETPM policy editor, select “Any port” as the Source Port and Destination Port in the Network Set Point A and Network Set Point B areas.
- If you require a port-based policy, increase the PMTU on the ETEPs to avoid packet fragmentation.

Solving Network Connectivity Problems

If traffic is not being passed and it is not due to policy priority errors, you might have problems with network connectivity, which can prevent new keys from being distributed to the PEPs before the old keys expire.

To avoid this, for each of your primary policies, create a secondary policy that targets the same traffic and set the **Renew keys/Refresh lifetime** to zero (0). The zero value assures that the keys never expire. Assign this policy a lower priority than the primary policy. If the keys for the primary policy on the PEP expire before new keys arrive, the secondary policy takes affect. Traffic continues to flow and stays secure until the connectivity issues are resolved and the PEPs receive new keys for the primary policy.

When you have a connectivity problem, start ETPM and click **Refresh Status** . If the status shown in the Policy View returns a  indicator, the interruption may have been temporary. In this case, you can re-establish the keys by clicking **Renew Keys**  from the ETPM.

When you have a network connectivity problem and a PEP status indicator returns an error, you can locate the affected communication link by checking log files.

- For ETPM to ETKMS communications errors, check the ETEMS or ETPM application log for an error entry as described in [“ETPM Log Files” on page 241](#).
- For ETKMS to PEP communications errors, check the ETKMS log files as described in [“ETKMS Log Files” on page 241](#).

Modifying EncrypTight Timing Parameters

Depending on the deployment, the default timing parameters for communications between EncrypTight components may need to be adjusted. These include parameters that control how long the ETPM waits for replies from the ETKMS, as well as how long the ETKMS waits for replies from the PEPs. Other timing parameters exist as well.

The amount of time that ETPM waits for a response from a ETKMS during a policy deployment can be changed by setting a value in the `config.ini` file. This file is located in the `configuration` directory inside the ETEMS installation directory. To change the value, add or edit the following line:

```
maxRetryWaitTime=xxx
```

Where `xxx` is the number of seconds that ETPM waits for a reply from a ETKMS. The default value is 6 minutes (360 seconds). The `maxRetryWaitTime` for ETPM should be set to a value at least 1 or 2 minutes longer than the value of the `retryStatusCheckTime` parameter on the ETKMS. This ensures that ETPM will wait for a reply from the ETKMS at least as long as the ETKMS waits for replies from the PEPs.

To set the `retryStatusCheckTime` parameter, edit the `kdist.properties` file. On an external ETKMS the file is located in the `/opt/etkms/conf` directory; on the local ETKMS it is located in `\tools\ETKMS\bin` (relative to the install directory). For information on timing parameters for a ETKMS, see [“Modifying the ETKMS Properties File” on page 255](#).

Certificate Implementation Errors

When you use certificates for TLS communications between the ETPM and the ETKMSs and between the ETKMSs and the PEPs, you might encounter the following problems.

- Cannot communicate with a PEP
- Keystore password might not be correct
- Certificates might not be valid yet
- Certificate might be missing or uninstalled

These errors can occur when you start the ETKMS server or when ETPM first tries to communicate with the PEP.

Cannot Communicate with PEP

If you attempt to add a new PEP to the ETEMS Appliance Manager after strict authentication is enabled in the EncrypTight software, you will receive a communications error. When strict authentication is enabled, the EncrypTight software cannot communicate with appliances that do not have the appropriate certificates.

To add a new PEP in a system configured to use strict authentication:

- 1 In the ETEMS preferences, temporarily disable strict authentication.
- 2 Add and configure the PEP.
- 3 Install certificates on the PEP and the re-enable strict authentication in ETEMS.
- 4 Refresh status.
- 5 If the status is okay, enable strict authentication on the PEP.

ETKMS Boot Error

If you entered the wrong password for the keystore when you set up the certificates, you can receive the error message “keystore was tampered with or password incorrect” when the ETKMS server starts. The error is recorded in the ETKMS log file. The keystore file on the ETKMS must be secured using the password specified in the `keystorePassword=myPassword` entry in the `kdist.properties` file.

Invalid Certificate Error

You can receive errors regarding invalid certificates if the time settings for the certificates and the EncrypTight components are significantly different.

If this occurs, check the `kdist.log` file on the ETKMS for the text:

```
Asynchronous invocation failed to (your PEP ip address here):  
javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake failure.
```

Check the time on your ETPM workstation, ETKMS servers, and PEPs. Compare these times with the time on the certificates. If the times between the EncrypTight components differ significantly, the certificate you installed on the PEP may not be valid yet.

You can check the validity by typing the following commands.

```
keytool -printcert -v -file <pep1.pem>  
or  
keytool -printcert -v -file <pep1.der>
```

Where “pep1.pem” or “pep1.der” is the name of the certificate file. Depending on the format of your certificate file, you might also be able to open up the file in a text editor and look for the line that says “Valid from.”

If your certificate is not valid yet, ensure that the time on the ETPM, ETKMSs, and PEPs is synchronized with an NTP server. Then either wait until your certificates are valid, or create a new certificate with the times set correctly.

Invalid Parameter in Function Call

Enabling strict authentication on a PEP before you install external certificates can cause communication issues. If you enable strict authentication on the ETEP before you install certificates, the management port locks up and rejects all communication from the management workstation and the ETKMSs.

To disable strict authentication on ETEPs:

- 1 Connect to the serial port of the appliance and open a terminal session.
- 2 Log in and type **configure** to enter configuration mode.
- 3 Type **management-interface** to enter management interface configuration mode.
- 4 Enter **strict-client-authentication disable**.

For example:

```
admin> configure

Entering configuration mode...

config> management-interface

Entering management interface configuration mode...

man-if> strict-client-authentication disable
```

For more information about using the `strict-client-authentication` command, see the *CLI User Guide* for the ETEP.

 **NOTE**

For information on enabling strict authentication and using certificates, see [“Using Enhanced Security Features” on page 261](#).

Part V Reference



19 Modifying the ETKMS Properties File

This section provides information about settings in the ETKMS properties file that you can use to control and optimize the performance of the ETKMS, including:

- [About the ETKMS Properties File](#)
- [Hardware Security Module Configuration](#)
- [Digital Certificate Configuration](#)
- [Logging Setup](#)
- [Base Directory for Storing Operational State Data](#)
- [Peer ETKMS and ETPM Communications Timing](#)
- [Policy Refresh Timing](#)
- [PEP Communications Timing](#)

About the ETKMS Properties File

For local ETKMSs, the ETKMS properties file `kdist.properties` is located in the `\tools\kdist\bin` directory, relative to the EncrypTight installation directory.

The ETKMS properties file `kdist.properties` is located in the `/opt/etkms/conf` directory. This file is divided into the following sections:

- Digital certificate configuration
- Logging setup
- Base directory for operational state data
- ETKMS/ETPM communications timing parameters
- Policy refresh timing
- General Communication Timing

NOTE

For external ETKMSs, all file locations defined are relative to the `/opt/etkms/bin` directory.

If you have physical access to the ETKMS, you can log in directly on the ETKMS server, or you can use an ssh client to log in remotely.

Hardware Security Module Configuration

The following entries control whether the encryption keys are stored in a Hardware Security Module (HSM).

```
# Hardware Security Module Configuration
hardwareModuleInUse=false
vaultBaseDir=../keys
```

To store the encryption keys in an HSM, set the `hardwareModuleInUse` entry to `true`. When the entry is set to `false`, the encryption keys are stored in the directory specified by the `vaultBaseDir` entry.

Digital Certificate Configuration

The following entries control digital certificate configuration and remote user certificate authorization. If you use smart cards such as the DoD Common Access Card, you need to enable both strict authentication and common name authorization in the ETKMS properties file.

```
# Certificate configuration
keystore=etkms.keystore
keystorePassword=myPassword
strictCertificateAuth=false
enableCNAuthCheck=false
cnAuthFilePath=../keys/cnAuth.cfg
```

Strict certificate authentication and common name authorization checking are disabled by default (`false`). To enable those features, change the values to `true`. The path for the common name authorization file is the default, but you can store the file in any directory on the ETKMS and enter the appropriate path here.



CAUTION

Modify only these parameters as part of enabling strict authentication and using certificates. For more information on strict authentication and using certificates, see [“Using Enhanced Security Features” on page 261](#). Modify other parameters only as instructed by a qualified support person.

Logging Setup

The following entries setup the Java log4j logging mechanism. By default the logging is setup for daily log files.

```
# Logging Setup
log4j.rootLogger=ALL, Daily
log4j.appender.R.Threshold=INFO
log4j.appender.R=org.apache.log4j.DailyRollingFileAppender
log4j.appender.R.DatePattern='.' yyy-MM-dd
log4j.appender.R.File=/var/log/etkms/kdist.log
log4j.appender.R.MaxFileSize=100KB
```

```

log4j.appender.R.layout=org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern=%d [%t] %-5p %c - %m%n

## Console logging
#log4j.rootLogger=ALL,stdout
#log4j.appender.stdout.Threshold=INFO
#log4j.appender.stdout=org.apache.log4j.ConsoleAppender
#log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
#log4j.appender.stdout.layout.ConversionPattern=%d %t %-5p %c - %m%n

```

Base Directory for Storing Operational State Data

This entry defines the database for storing the keys and current metapolicies.

```

# Base directory for storing operational state data
KeyDistDbLoc=..

```

Peer ETKMS and ETPM Communications Timing

The following entries define the communications timing between the ETKMS and peer ETKMSs and the ETKMS and the ETPM.

```

#### KeyDist/ETPM Communications Timing
# Wait for peer key after deploy (1-1200 Seconds)
waitForPeerKeyTime=30

# Time to wait for status check to complete (1-3600 Seconds)
retryStatusCheckTime=315

# Check for message period in milliseconds (20-3000 mS)
recheckMessageWaitTimeMS=1000

# Time to wait for additional keys from peer KeyDist after key is received in
seconds (1-1200 S)
waitForReceivedKeyTime=5

```

waitForPeerKeyTime	Specifies in seconds how long the ETKMS waits to get any keys from other peer ETKMSs.
retryStatusCheckTime	Specifies in seconds the time the ETKMS waits to receive status from PEPs. If the status is not received from a PEP within the defined time, an error status indication appears on the ETPM screen next to the appropriate PEP.
recheckMessageWaitTimeMS	Specifies in milliseconds the elapsed time the ETKMS waits to check for a command from the ETPM.
waitForReceivedKeyTime	Specifies in seconds how long the ETKMS should wait for additional keys from a peer ETKMS.

Policy Refresh Timing

The policy refresh timing controls the timing between the initiation of a renew keys and policy lifetime and the deletion of the expired keys. The following entries specify the timing for the policy refresh.

```
#### Policy refresh timing
# Policy refresh delete delay (1-120 minutes)
minutesAfterRefreshExpireBeforeDelete=30

# Policy refresh buffer for daily refresh (1-120 minutes)
maxBufferMinutesBeforeDailyRefresh=20

minutesAfterRefreshExpireBeforeDelete Specifies in minutes the time the PEP waits after a
Refresh before it deletes the old keys.

maxBufferMinutesBeforeDailyRefresh Specifies in minutes the earliest time in which a
Refresh is issued.
```

PEP Communications Timing

The following parameters define the ETKMS to PEP communications timing.

```
#### General Communication Timing
# Initial wait (1-1200 Seconds)
initialRetryWaitTime=300

# Retry wait (1-1200 Seconds)
retryWaitTime=300

# Retry count (1-100)
retryCount=1

# Max retry wait (1-1200 Seconds)
maxRetryWaitTime=300

#### PEP Extended Communication Timing
# Initial PEP retry wait (1-1200 Seconds)
initialPEPRetryWaitTime=360

# PEP retry count before starting final wait (1-100)
initialPEPRetryCount=12

# Final PEP retry wait (1-1200 Seconds)
finalPEPRetryWaitTime=600
```

These entries divide the timing into general communications timing and extended communications timing.

The general timing defines a group of communication attempts defined by `retryCount`. The time between the first communication attempt and the second is defined by the `initialRetryWaitTime`. The time between the second and third attempt is defined by `maxRetryWaitTime`. This continues for `n` communications attempts as defined by `retryCount` or until `maxRetryWaitTime` is reached. This process is repeated as defined by the extended communications parameters.

Once the n^{th} retry (defined by `retryCount`) is unsuccessful, the ETKMS waits a period of time defined by `initialPEPRetryWaitTime` when it then repeats the communication attempts as defined by the general timing parameters. This repeats for n times as defined by `initialPEPRetryCount`. If the communication is still unsuccessful, the ETKMS waits a period of time defined by `FinalPEPRetryWaitTime` and then attempts to communicate as defined by the general parameters and keeps repeating this process until communications are established or until another policy is deployed to the PEP.

20 Using Enhanced Security Features

This section includes the following topics:

- [About Enhanced Security Features](#)
- [About Strict Authentication](#)
- [Using Certificates in an EncrypTight System](#)
- [Changing the Keystore Password](#)
- [Configuring the Certificate Policies Extension](#)
- [Working with Certificates for EncrypTight and the ETKMSs](#)
- [Working with Certificates and an HSM](#)
- [Working with Certificates for the ETEPs](#)
- [Validating Certificates](#)
- [Enabling and Disabling Strict Authentication](#)
- [Removing Certificates](#)
- [Using a Common Access Card](#)

About Enhanced Security Features

EncrypTight provides a number of features that you can use to increase system security. These features are disabled by default, but available for your use. Some of these features are specific to the operation of the ETEPs, while others affect system-wide EncrypTight operations. Enhanced security features include:

- FIPS mode

Federal Information Processing Standards are security standards that govern the use of computer systems in non-military U.S. government agencies and contractors. When ETEPs operate in FIPS mode, only specific encryption and authentication algorithms are accepted. To learn more about ETEPs and FIPS mode, see [“FIPS Mode” on page 331](#).

- IPsec on the management interface

By default, communication between the management workstation and the ETEPs is secured using SSH and TLS. You can provide additional security for EncrypTight management communications by using IPsec policies on the management ports instead. This feature is controlled through the command line interface for the ETEP. To learn more about creating IPsec policies for the ETEP management ports, refer to the *ETEP CLI User Guide*.

- Strong password enforcement

ETEPs with software version 1.6 or later can be configured to use strong password enforcement. The conventions used with strong password enforcement are far more stringent than those used with the default password management. To learn more about strong password enforcement, see [“Configuring the Password Enforcement Policy” on page 103](#).
- Strict authentication

With strict authentication, all communications between EncrypTight components is authenticated using certificates. To learn more about strict authentication and using certificates see [“About Strict Authentication” on page 262](#).
- Hardware Security Module

A hardware security module (HSM) is available as an option for your ETKMSs. HSMs provide tamper-proof storage for encryption keys and certificates. To learn more about working with an HSM, see [“Working with Certificates and an HSM” on page 275](#).
- Common Access Cards

EncrypTight supports the use of smart cards such as the Common Access Cards used by the U.S. Department of Defense. The use of smart cards provides user authorization in addition to certificate-based authentication. To learn more, see [“Using a Common Access Card” on page 294](#).

About Strict Authentication

EncrypTight uses the Transport Layer Security (TLS) protocol for secure communication between the different components of the system (the management workstation, the ETKMS, and the PEPs). EncrypTight can use either:

- TLS with encryption only
- TLS with encryption and strict authentication enabled

When strict authentication is enabled, all TLS communications between EncrypTight components is authenticated using certificates. Authenticating the communications between components provides an extra level of security. Optionally, you can also set up the system to validate certificates by checking Certificate Revocation Lists (CRLs) or by using the Online Certificate Status Protocol (OCSP).

Strict authentication is available for ETEPs with software version 1.6 or later. Strict authentication is disabled by default. After you install certificates on all of the devices that you are going to use, you can enable strict authentication.



Do not enable strict authentication before you install certificates on all of the EncrypTight components. Doing so can lead to errors and communication failures.

A *certificate* is an electronic document that contains a public key that corresponds to the private key of the entity named as the subject of the certificate. Certificates can be generated by the entity itself (self-signed) or they can be issued by a certificate authority (CA). A CA is a trusted organization that authenticates certificate applications, issues and revokes certificates, and maintains status information about certificates. CA-signed certificates help establish a chain of trust. Keys and certificates are stored in an encrypted, password-protected keystore.

Related topics:

- [“Prerequisites” on page 263](#)
- [“Order of Operations” on page 263](#)
- [“Certificate Information” on page 264](#)
- [“Changing the EncrypTight Keystore Password” on page 266](#)
- [“Configuring the Certificate Policies Extension” on page 269](#)
- [“Validating Certificates” on page 287](#)
- [“Enabling and Disabling Strict Authentication” on page 292](#)

Prerequisites

An important prerequisite to installing new certificates is identifying the certificate authority you plan to use. Your organization may have a standard CA that everyone uses, or you may need to select one for this particular security application. The information in this chapter assumes that you have established a relationship with a certificate authority.

In order to follow the procedures discussed in this section and work with certificates in an EncrypTight system, you need to understand how to do several tasks covered in more detail in other sections. Cross references to those sections are provided in [Table 67](#).

Table 67 Prerequisites for Using Certificates with EncrypTight

How to:	Reference:
Navigate and work with ETEMS	“Getting Started with ETEMS” on page 83
Add and configure PEPs	“Provisioning Appliances” on page 95
Access the command line interface on the ETKMS	“Logging Into the ETKMS” on page 47
Access the command line interface for a PEP	See the configuration chapter for the model of PEP that you are using.

NOTE

If you plan to operate in FIPS mode, make sure you enable FIPS mode first and push the configuration to the ETEPs before you begin to install certificates and set up strict authentication. If you enable FIPS mode after strict authentication has been activated, you will need to reinstall your certificates.

Order of Operations

You should proceed with caution as you enable strict authentication in your deployment. Among the issues you could encounter are invalid, misconfigured, or expired certificates that cause communication failures. The following order of operations is recommended:

- 1 If you plan to operate in FIPS mode, enable FIPS mode on your ETEPs before you make other changes.
- 2 Change the keystore password for the EncrypTight software and the ETKMSs.
- 3 Install certificates and keys on the management workstation and a few PEPs.

- 4 Temporarily enable strict authentication in ETEMS and make sure that you can still communicate with the PEPs (refresh status for the PEPs that you used in step 3. If the PEPs respond appropriately, continue with the next step. If you cannot communicate with the PEPs, troubleshoot and fix the problems found.
- 5 If step 4 was successful, enable strict authentication on the PEPs that you used in step 3 and retest communications. If ETEMS can still communicate with the PEPs, then ETEMS has certificates that can be used.
At this point, you can disable strict authentication and continue to provision more of the network.
- 6 When you have installed certificates on all of the devices in the system (including the ETKMSs and all of your PEPs), you can reenable strict authentication in ETEMS.
- 7 Refresh status for all devices to verify that ETEMS can still communicate with all devices. If you cannot communicate with a device, it probably has an invalid or misconfigured certificate.
Fix any issues discovered and proceed.
- 8 Enable strict authentication on all of the PEPs.
- 9 Enable strict authentication on the ETKMSs.

NOTE

If you need to add a new PEP after you have enabled strict authentication, temporarily disable strict authentication in the ETEMS preferences first, and then add the PEP. Configure the PEP as needed. After you push the configuration, install certificates on the PEP and re-enable strict authentication in ETEMS. Refresh status to test the communications and if everything is successful, enable strict authentication on the new PEP.

Related topics:

- [“Prerequisites” on page 263](#)
- [“Certificate Information” on page 264](#)
- [“Using Certificates in an EncrypTight System” on page 265](#)

Certificate Information

When you generate a keypair and create certificates, you must provide information that uniquely identifies the device. This information is referred to as a *distinguished name* and consists of the values described in [Table 68](#). When you generate a keypair using the keytool utility, this information is specified as part of the `-dname` parameter.

Table 68 Distinguished name information

Setting	Description
Common Name (CN)	A name that identifies the device or person. Length: 0-64 characters.
Organizational Unit (OU)	Name of a sub-section of the organization, such as a department or division. Length: 0-64 characters.
Organization (O)	Organization or company name. Length: 0-64 characters.
Locality (L)	City, town, or geographical area where the organizational unit is located. Length: 0-128 characters.
State/Province (S)	State or province where the organizational unit is located. Length: 0-128 characters.
Country (C)	Two letter country abbreviation (optional).

In usage, you type this string as follows:

```
-dname "cn=<common name>, ou=<organization unit>, o=<organization name>,  
l=<location>, s=<state/province>, c=<country>"
```

The information must be entered in the order shown. For example:

```
-dname "cn=John Doe, ou=customer support, o=my company, l=raleigh, s=NC,  
c=US"
```

Related topics:

- [“Generating a Key Pair” on page 272](#)
- [“Generating a Key Pair for use with the HSM” on page 276](#)
- [“Working with Certificate Requests” on page 281](#)

Using Certificates in an EncrypTight System

EncrypTight components ship with self-signed identity certificates. You can continue to use these certificates, or you can replace them with certificates acquired from a trusted CA. By default, EncrypTight uses the Transport Layer Security (TLS) protocol for communications between components. This encrypts communications, but does not automatically provide authentication. If you enable strict authentication, you can use certificates to authenticate identities and set up encrypted communications for management traffic between components.

To authenticate the communications, each component needs one of the following:

- A copy of the identity certificate for every component with which it communicates.
- A trusted root CA. EncrypTight components can check up to 10 certificates in a certificate chain.

Manually exporting and installing certificates for a large number of devices can be burdensome. In larger deployments it is more efficient to use a CA certificate than to install individual certificates for each component with which a device might need to communicate.

When you replace the self-signed certificates, each component in an EncrypTight system needs at least an identity certificate for itself and a copy of the trusted CA certificate. The CA certificate is used to validate the identity certificate when communication sessions are initiated. You might also need certificates for any intermediate CAs in the chain.

You request and install certificates for the EncrypTight software and the ETKMS using the java-based keytool utility. For the ETEP PEPs, you can use the Certificate Manager perspective in ETEMS to request and install certificates (for more information, see [“Working with Certificates for the ETEPs” on page 277](#)).

Related topics:

- [“About Strict Authentication” on page 262](#)
- [“Working with Certificates for EncrypTight and the ETKMSs” on page 272](#)
- [“Working with Certificates and an HSM” on page 275](#)
- [“Working with Certificates for the ETEPs” on page 277](#)
- [“Validating Certificates” on page 287](#)

Changing the Keystore Password

Before you begin using certificates, you need to change the default passwords for the EncrypTight keystore and the ETKMS keystore. This section includes the following topics:

- [“Changing the EncrypTight Keystore Password” on page 266](#)
- [“Changing the ETKMS Keystore Password” on page 266](#)

Changing the EncrypTight Keystore Password

The keystore is where keys and certificates used by ETEMS are securely stored. The contents of the keystore are password protected. We recommend changing the default password of **admin123**.

Other operational notes that you should be aware of:

- Always use ETEMS to change the keystore password. Using keytool to change the keystore password can cause communication errors between ETEMS and EncrypTight appliances, because keytool does not inform ETEMS of password changes.
- The keystore is located in `<installDir>\cvConfig\keys`, where `<installDir>` is the top-level EncrypTight directory. Use this directory when adding certificates to the keystore.
- ETEMS reads the keystore upon startup. It does not act on new certificates added to the keystore while ETEMS is running. ETEMS needs to be restarted for changes to take effect.
- When uninstalling EncrypTight, the keystore is saved along with the workspace.

Keystore password conventions are as follows:

- 6-256 characters
- Case sensitive
- All standard keyboard characters are allowed

To change the EncrypTight keystore password:

- 1 On the **Edit** menu, click **Change Keystore Password**.
- 2 Enter the new password.
- 3 Reenter the new password, and click **Apply**. The vault keystore password and the passwords guarding the private and secret keys are changed to the new value.

Related topics:

- [“Changing the ETKMS Keystore Password” on page 266](#)

Changing the ETKMS Keystore Password

The procedure for changing the keystore password on a ETKMS depends on whether or not the ETKMS includes an HSM. This section includes the following topics:

- [“Changing the Keystore Password on a ETKMS” on page 267](#)
- [“Changing the Keystore Password on a ETKMS with an HSM” on page 268](#)

Changing the Keystore Password on a ETKMS

Changing the password on a ETKMS involves multiple steps, including:

- 1 Stop the ETKMS service
- 2 Use keytool to change the password
- 3 Change the password for each individual key stored
- 4 Change the password listed in the ETKMS properties file
- 5 Restart the ETKMS service

Stopping the ETKMS Service

To stop the ETKMS service:

- 1 Open an SSH session and log into the ETKMS.
- 2 At the command line, enter


```
service etkms stop
```

Change the Password Used by Keytool

Use the keytool utility to change the password of the keystore. The default password for the ETKMS keystore is **g3h31m**.

To change the keystore password on the ETKMS:

- 1 Open an SSH session and log into the ETKMS.
- 2 At the command line, enter


```
keytool -storepasswd -new <NewPassword> -keystore etkms.keystore -storepass <CurrentPassword>
```

The new password must be at least 6 characters long. If you do not specify the current password on the command line, you will be prompted for it.

NOTE

If you change the password for the keystore that keytool uses, you must also change the password used by the ETKMS software. If the keystore password and the password stored in the ETKMS properties file do not match, errors will be logged and the ETKMS will be unable to generate and renew encryption keys. For instructions on changing the password stored in the ETKMS properties file, see ["Changing the Password Used in the ETKMS Properties File"](#) on page 268.

Change the Password for Individual Keys

You also use the keytool utility to change the password for each key stored.

To change the password for individual keys:

- 1 List the keys with passwords that need to be changed by typing:


```
keytool -list -keystore etkms.keystore -storepass <KeyStorePassword>
```
- 2 For each key, change the password with the following command using the appropriate alias (the first name on each line in the results from the command above):


```
keytool -keypasswd -keystore etkms.keystore -storepass <KeyStorePassword> -keypass <OldKeyPassword> -new <NewKeyPassword>
```

Changing the Password Used in the ETKMS Properties File

The ETKMS properties file includes an entry for the keystore password that the ETKMS software uses for functions that access the keystore.

To change the password listed in the ETKMS properties file:

- 1 Use a text editor to edit the file
`/opt/etkms/conf/kdist.properties`
- 2 Find the section labelled "Certificate configuration" and enter the new password for the `keystorePassword` entry.

For example:

```
# Certificate configuration
keystore=etkms.keystore
keystorePassword=myPassword
```

NOTE

If you change the password stored in the ETKMS properties file, you must also change the password for the keystore that is used by the keytool utility. If the keystore password and the password stored in the ETKMS properties file do not match, errors will be logged and the ETKMS will be unable to generate and renew encryption keys. For instructions on changing the password used by keytool, see ["Change the Password Used by Keytool" on page 267](#).

Restart the ETKMS Service

To start the ETKMS service:

- 1 Open an SSH session and log into the ETKMS.
- 2 At the command line, enter
`service etkms start`

Changing the Keystore Password on a ETKMS with an HSM

The HSM uses two passwords, one for the Security Officer role, and one for a User role. On the ETKMS, these are set to the same value. In order to change the password, you must use the `HSMPwdChg.sh` script.

To change the HSM password:

- 1 Switch to the `/opt/etkms/bin` directory by typing:
`cd /opt/etkms/bin`

- 2 Type:
`./HSMPwdChg.sh`

This will print out the value of the current password, based on the contents of the `coLicense.properties` file. Make note of this value. You will need to provide it when you change the passwords.

- 3 Using a text editor, open the `coLicense.properties` file and change the current value of `etkmsLicense` property.
- 4 Obtain the new password by typing:

```
./HSMPwdChg.sh
```

The script will print out the new value of the password. Make note of this value.

- 5 Change the password for the Security Officer role by typing:

```
ctkmu p -O
```

You will be prompted for the value of the old password and then for the value of the new password.

- 6 Change the password for the User role by typing:

```
ctkmu p
```

You will be prompted for the value of the old password and then for the value of the new password.



NOTE

The documentation provided by the manufacturer of the HSM refers to these passwords as PINs.

Configuring the Certificate Policies Extension

EncrypTight supports the use of the certificate policies extension in certificates. CAs use this extension to indicate the purposes for which a certificate was issued, for example, digitally signing e-mail or encryption. If a certificate is being used for a purpose that is not indicated by the extension, it can be rejected.

In a certificate, the certificate policies extension indicates the purposes for which a certificate was issued with one or more registered Object Identifiers (OIDs), which are values that can vary by organization and industry. If the CA that issues the certificate does not want to limit the purposes for which the certificate can be used, they can use a special OID that indicates it can be used for any policy.

If your organization uses the certificate policies extension in certificates, you need to specify the OIDs that will be accepted by the EncrypTight software, the ETKMSs, and each ETEP before you begin requesting and installing certificates. The OIDs are ignored until you enable strict authentication.

You can configure the certificate policies extension for ETEPs on the Advanced tab of the Appliance Editor. The changes do not take effect until you push the configurations to the ETEPs.

To configure the certificate policies extension for ETEPs:

- 1 In Appliance editor for the ETEP, click the **Advanced** tab.
- 2 Click **Enable Policy Extensions**.
- 3 Click **Add**.
- 4 In the Certificate Policy Extension editor, type the OID that you want to add and click **OK**.
 - If you make a mistake, select the OID in the list and click **Modify** to change it.
 - If you need to remove an OID, select it and click **Delete**.
- 5 Repeat steps 3 and 4 for each OID you need to add.
- 6 Click **Save**.

**TIP**

If you are deploying numerous ETEPs, you can save time by modifying the default configurations for the ETEP models that you use. For more information about modifying default configurations, see [“Working with Default Configurations” on page 110](#).

You configure the certificate policies extension for ETKMSs by adding the OIDs to the ETKMS properties file. The ETKMS properties file `kdist.properties` is located in the `/opt/etkms/conf` directory.

To configure certificate policy extensions for ETKMSs:

- 1 Log in as root and edit the file `/opt/etkms/conf/kdist.properties` and add or edit the following lines in the Certificate Configuration section:

```
certificatePolicy<n>=<OID>
```

You can add as many lines as you need. Refer to [Table 69](#) for an explanation of the parameters used.

- 2 Save and close the file.
- 3 Restart the ETKMS by typing:

```
service etkms restart
```

Table 69 ETKMS Certificate Policies Entries

Parameter	Description
n	An integer beginning with 1. If you need to add multiple lines, number them consecutively. You cannot skip numbers.
OID	The OID of the certificate policy, entered as a series of integers separated by periods. For example: <pre>certificatePolicy1=1.3.5.8</pre> <pre>certificatePolicy2=1.3.5.10.64</pre>

You can configure the certificate policies extension for EncrypTight in the EncrypTight Preferences. These changes take effect immediately.

To configure certificate policies extension for the EncrypTight:

- 1 In EncrypTight, select **Edit > Preferences**.
- 2 Click **ETEMS** to expand the tree and then click **Communications** (see [Figure 95](#)).
- 3 Click **Enable Certificate Policy Extensions**.
- 4 Click in the **Certificate Policy Extension OIDs** box and type the OIDs you need to use, separating each with a comma.
- 5 Click **Apply** and then click **OK**.

Figure 95 Communications Preferences

About the Policy Constraints Extension

The certificate policies extension can be used in conjunction with the policy constraint extension. This extension is configured by your CA and requires no setup in EncrypTight components. It places additional controls on how certificates can be used. The policy constraints extension can:

- Prohibit policy mapping

Policy mapping is the practice by which one OID is considered equivalent to a different OID. When policy mapping is prohibited, a value in the extension indicates the number of additional certificates in the chain that can be checked before policy mapping is prohibited. Beyond that point, policy mapping is not allowed and authentication can fail.
- Require that every certificate in the certificate chain include acceptable policy identifiers, as specified in the certificate policies extension

With this option, a value in the extension indicates the number of additional certificates in the chain that can be checked before all certificates in the chain must include acceptable policy identifiers, either an exact match to an OID configured in the device or an OID considered equivalent through policy mapping. If the next certificate in the chain does not include acceptable OIDs, authentication can fail.

Your CAs can provide information about their practice for using these extensions.

Related topics:

- [“Working with Certificates for EncrypTight and the ETKMSs” on page 272](#)
- [“Working with Certificates and an HSM” on page 275](#)
- [“Working with Certificates for the ETEPs” on page 277](#)
- [“Enabling and Disabling Strict Authentication” on page 292](#)

Working with Certificates for EncrypTight and the ETKMSs

For both the workstation running the EncrypTight software and the ETKMS, use the *keytool* utility to request and install certificates. The *keytool* utility is a Java-based utility for key and certificate management. A complete discussion of using the *keytool* utility is beyond the scope of this guide. You can find additional information on the Internet.

On each EncrypTight component, encryption keys and certificates are stored in the keystore. The location of the *keytool* utility and the keystore depends on the component with which you are working.

- On the management workstation, *keytool* is located in `<installDir>\jre\bin` where `<installDir>` is the directory where you installed the EncrypTight software. By default, keys are stored in the keystore located in the `<installDir>\cvConfig\keys` directory.
- On the ETKMS, *keytool* is located in `/usr/java/latest/bin/keytool` and the keystore is located in `/opt/etkms/keys`.

You need to follow the procedures in this section for both the management workstation and the ETKMS. Before proceeding, you should change the default password for the keystore (see [“Changing the Keystore Password” on page 266](#)). If your organization uses the certificate policies extension for certificates, you also need to specify what values are valid for this extension on each device (see [“Configuring the Certificate Policies Extension” on page 269](#)).

If you plan to use a CA certificate as an external certificate for validation, obtain a copy of the CA certificate before you begin. You will receive a .PEM or .DER file that you can import into the keystore on the devices with which you work.

NOTE

If your ETKMS includes an HSM, skip this section and follow the instructions in [“Working with Certificates and an HSM” on page 275](#) to generate requests and install certificates.

This section includes the following topics:

- [“Generating a Key Pair” on page 272](#)
- [“Requesting a Certificate” on page 273](#)
- [“Importing a CA Certificate” on page 274](#)
- [“Importing a CA Certificate Reply” on page 274](#)
- [“Exporting a Certificate” on page 275](#)

Generating a Key Pair

To request a certificate from a CA, you must first generate a public/private key pair. This procedure essentially creates a self-signed certificate and places it in the keystore.

To generate a key pair:

- 1 From the command line, use the following command to generate a public/private key pair:

```
keytool -genkeypair -dname {"cn=<Entity Name>, ou=<Organizational Unit>,
o=<Organization>, c=<Country>"} -alias <alias> -keypass <key password>
-keystore <keystore> -keyalg <algorithm> -storepass <password>
-validity <n>
```

Table 70 Keytool genkeypair Command

Parameter	Description
dname	The distinguished name parameters for the certificate. For information about this parameter, refer to “Certificate Information” on page 264 .
alias	The name of the keystore entry.
keypass	The password for the private key.
keystore	The name and location of the keystore.
keyalg	The algorithm used to generate the keys.
storepass	The password for the keystore.
validity	The number of days for which the certificate entry is valid.

For example:

```
keytool -genkeypair -dname "cn=ETKMS3, ou=Storage o=MyCompany c=US"
-alias Cert1 -keypass password1 -keystore C:\Safe\mykeystore -keyalg RSA
-storepass password2 -validity=180
```

This would generate a keypair and self-signed certificate for the entity named “ETKMS3” in the organizational unit of “Storage,” part of the organization “MyCompany,” in the United States. The alias of the certificate is “Cert1” and it is valid for 180 days.

Requesting a Certificate

Using the `keytool -certreq` command, create a certificate request to be sent to your CA.

To create the certificate request:

- 1 From the command line, use the following command to generate a certificate request:

```
keytool -certreq -file <filename>
```

Where `filename` is the name of the certificate signing request. You must use the filename extension of `.csr`.

- 2 When prompted, enter the keystore password.
- 3 Using the procedure require by your CA, send the CSR file to your CA.

For example:

```
keytool -certreq -file ETKMS3.csr
```

This creates a certificate request file names “ETKMS3.csr” that you can send to your CA.

Importing a CA Certificate

Depending on the CA that you use, you could receive a single certificate or a certificate chain. If the reply is a single certificate and it is not a copy of a CA trusted root certificate, you need acquire the certificate for a trusted root. If the reply from the CA is a chain itself, you only need the root, or top-level certificate in the chain.

If the trusted root certificate is not a file by itself, copy and paste it to a new file.

Use the `keytool` command to install the trusted root certificate from the CA into the keystore for the EncrypTight software. The CA certificate can be used to validate the public key of the CA that you use.

To install a CA certificate:

- 1 From the command line, import the CA certificate into the keystore with the `keytool -import` command.

```
keytool -importcert -alias <alias> -file <filename> -keystore
<keystore> -storepass <password>
```

Table 71 Keytool Parameters for Importing a CA Certificate

Parameter	Description
alias	The name of the entry for this certificate in the keystore.
file	The name and location of the certificate file.
keystore	The name and location of the keystore file.
storepass	The password for the keystore.

For example:

```
keytool -importcert -alias CACert -file C:\docs\CACart.cer
-keystore C:\Safe\mykeystore -storepass password2
```

This imports the CA certificate into the keystore.

Importing a CA Certificate Reply

Once you have a certificate of the CA to which you submitted your certificate signing request, you can import the certificate reply from the CA.

To import a CA certificate reply:

- 1 From the command line, use the following command to import the certificate:

```
keytool -importcert -trustcacerts -file <filename>
```

Where `filename` is the name of the certificate file that you want to import.

For example:

```
keytool -importcert -trustcerts -file c:\docs\ETKMS3.cer
```

This imports the certificate file named “ETKMS3.cer” into the keystore.

Exporting a Certificate

For other devices to authenticate the identity of an entity, they might need a copy of the entity's certificate. You can use the `keytool export` command to export certificates for this purpose.

To export a certificate:

- 1 From the command line, use the following command to export a copy of the certificate:

```
keytool -exportcert -alias <alias> -file <filename>
```

Table 72 Keytool Export Parameters

Parameter	Description
alias	The name of the entry for this certificate in the keystore.
filename	The name of the file that you want to export.

For example:

```
keytool -exportcert -alias ETKMS3Cert -file ETKMS3.cer
```

This exports a copy of the certificate with the alias “ETKMS3Cert” to a file named “ETKMS3.cer.”

Working with Certificates and an HSM

If you purchased an HSM to use with your ETKMS, requesting and installing certificates requires utilities specific to the software that runs the HSM, as well as `keytool` commands. The procedures are similar to those discussed in [“Working with Certificates for EncrypTight and the ETKMSs” on page 272](#), but the commands require specific settings.

Before proceeding, you should review the concepts discussed previously in this chapter.

This section includes the following topics:

- [“Configuring the HSM for Keytool” on page 275](#)
- [“Importing CA Certificates into the HSM” on page 276](#)
- [“Generating a Key Pair for use with the HSM” on page 276](#)
- [“Generating a Certificate Signing Request for the HSM” on page 277](#)
- [“Importing Signed Certificates into the HSM” on page 277](#)

Configuring the HSM for Keytool

Use the following command to configure the HSM to work with the `keytool` utility.

To configure the HSM to work with `keytool` commands:

- 1 At the command line, type:

```
etconf -fc
```

Importing CA Certificates into the HSM

To import CA certificates into the HSM:

- 1 To import a CA certificate, at the command line type:

```
ctcert i -f <filename> -l <alias>
```

- 2 To set the certificate as trusted, type:

```
ctcert t -l <alias>
```

- 3 If prompted, enter the HSM password.

Table 73 ctcert Parameters

Parameter	Description
filename	The name of the certificate file that you want to import.
alias	The name of the entry for this certificate in the HSM.

Generating a Key Pair for use with the HSM

To generate a key pair for use with the HSM:

- 1 At the command line, type:

```
keytool -keystore NONE -storetype PKCS11 -genkey -keyalg RSA
-providername SunPKCS11-psie -alias <alias> -storepass <password>
-dname "<distinguished name>"
```

Table 74 Generating an HSM key pair with keytool

Parameter	Description
keystore	Specifies the keystore to use. A type of NONE indicates that a security device is being used for the keystore.
storetype	Specifies the type of keystore in use.
genkey	Generates a key pair.
keyalg	Specifies the algorithm to use for the key pair.
providername	Specifies the name of the security device/software.
alias	Assigns a name for this key pair in the keystore.
storepass	Specifies the password for the keystore.
dname	Assigns values to the distinguished name fields for the certificate. For information about this parameter, refer to "Certificate Information" on page 264 .

Generating a Certificate Signing Request for the HSM

To generate a certificate signing request:

- 1 At the command line, type:

```
keytool -keystore NONE -storetype PKCS11 -certreq -keyalg RSA
-providername SunPKCS11-psie -alias <alias> -storepass <password> -file
<csr filename>
```

Table 75 Generating a Certificate Signing Request for use with the HSM

Parameter	Description
keystore	Specifies the keystore to use. A type of NONE indicates that a security device is being used for the keystore.
storetype	Specifies the type of keystore in use.
certreq	Generates a certificate signing request.
keyalg	Specifies the algorithm to use for the certificate.
providername	Specifies the name of the security device/software.
alias	Assigns a name for this entry in the keystore.
storepass	Specifies the password for the keystore.
file	Specifies a name for the certificate signing request file.

Importing Signed Certificates into the HSM

To import signed certificates into the HSM:

- 1 At the command line, type:

```
keytool -keystore NONE -storetype PKCS11 -import -alias <alias> -file
<filename> -providername SunPKCS11-psie -storepass <password>
```


Table 76 Importing a certificate to the HSM

Parameter	Description
keystore	Specifies the keystore to use. A type of NONE indicates that a security device is being used for the keystore.
storetype	Specifies the type of keystore in use.
alias	Assigns a name for this entry in the keystore.
file	Specifies the name of the certificate file to import.
providername	Specifies the name of the security device/software.
storepass	Specifies the password for the keystore.
providername	Specifies the name of the security device/software.

Working with Certificates for the ETEPs

The Certificate Manager is a tool for obtaining and managing certificates for your ETEPs, including identity certificates and the external certificates used for validating other EncrypTight components.

To start the Certificate Manager do one of the following:

- In the Windows menu, click **Open**. In the list of perspectives, click **Certificate Manager**.
- On the Perspective tab in the upper right corner of the screen, click the Open Perspective button . In the list of perspectives, click **Certificate Manager**.

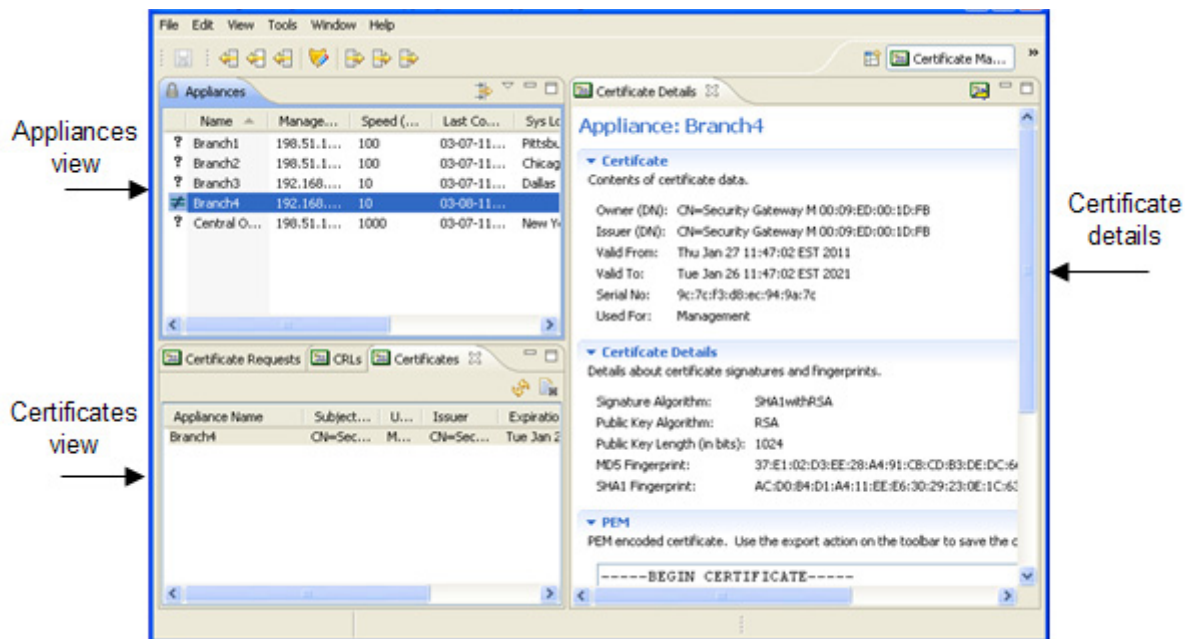
Related topics:

- [“Understanding the Certificate Manager Perspective” on page 278](#)
- [“Certificate Manager Workflow” on page 279](#)

Understanding the Certificate Manager Perspective

The Certificate Manager perspective has its own unique set of views and toolbars that are specific to managing certificates on EncryptTight appliances. Most tasks and actions are available through toolbar buttons and shortcut menus. To open a view's shortcut menu, right-click anywhere in the view.

Figure 96 Certificate Manager perspective



The Certificate Manager makes use of the following views:



- **Appliances view**
The Appliances view displays the appliances available to the Certificate Manager. To perform a certificate task on an appliance, select it in the Appliances view. Then use the shortcut menu or the toolbar button to select an action.
- **Certificates view**
The Certificates view shows certificates that are installed on selected appliances. The Certificates view shows a summary of the certificate and how its used (for management, peer authentication, or gateway). Use the shortcut menu to delete an external certificate, view certificate details, or export a certificate.
- **Certificate Requests view**

The Certificate Requests view displays pending certificate requests for selected appliances. You can manage certificate requests from the shortcut menu (view, delete, or install). Select a request from this view to see its contents in detail, including the PEM-formatted certificate request.

- CRLs view

The CRLs view displays Certificate Revocation Lists installed on the selected appliances. You can manage CRLs using the shortcut menu.

The Certificates view, Certificate Requests view, and the CRLs view provide the following options to manage the contents of the view:

- **Clear contents** removes certificate information from the view. This action does not affect the certificates or CRLs installed on an appliance. To clear the contents of the view, click .
- The **Refresh** action updates the certificate status for the appliances in the view. To refresh status, click Refresh on the shortcut menu or click .

Certificate Manager Workflow

An important prerequisite to installing new certificates is identifying the certificate authority you plan to use. Your organization may have a standard CA that everyone uses, or you may need to select one for this particular security application. The information in this chapter assumes that you have established a relationship with a certificate authority.

These are the typical tasks to perform to obtain and manage certificates:

- 1 Select a CA.
- 2 Obtain external certificates (CA certificate or certificates for other EncrypTight components).
- 3 Install external certificates.
- 4 Generate a certificate signing request and submit it to a CA.
- 5 Install the certificate.

Working with External Certificates

EncrypTight appliances use external certificates to validate communications from peers. An external certificate can be a CA certificate or a copy of the peer certificate itself. A minimum of one external certificate is required for peer authentication. You can install as many external certificates as are needed to validate the peers that communicate securely with the EncrypTight appliance.

Related topics:

- [“Obtaining External Certificates” on page 279](#)
- [“Installing an External Certificate” on page 280](#)

Obtaining External Certificates

If you plan to use a CA certificate as an external certificate you need to obtain one from a CA or use a CA certificate provided by your company. If you plan to use peer certificates as external certificates, you must install the identity certificate of each peer that will be communicating with the appliance.

 **NOTE**

The procedure for obtaining a CA certificate varies with each CA. These are the typical steps.

To obtain a CA certificate from a CA:

- 1 On the CA's website, complete the registration process.
- 2 Download the CA certificate from the CA's website.
- 3 In the Certificate Manager, install the CA certificate as an external certificate.

To use the peer appliance's identity certificate as an external certificate:

- 1 Export the certificate from the peer appliance.
- 2 Install the certificate file as an external certificate.

See the following topics for more information:

- [“Installing an External Certificate” on page 280](#)
- [“Exporting a Certificate” on page 286](#)

Installing an External Certificate

Use the following procedure to install a CA certificate or peer certificate as an external certificate. The external certificate must be a PEM encoded file.

To install an external certificate:

- 1 In the Appliances view, right-click the appliance on which to install the external certificate and click **Install External Certificate** in the shortcut menu.
- 2 In the Import Certificate window, browse to the location of the PEM encoded certificate file and select it.
- 3 Click **Open**.
- 4 In the Certificate Use window, click the option that represents the intended use of this certificate. In most cases, you will choose **Trusted Certificate for IPSec Peer Authentication**. Only select **OCSP Responder Certificate** if this is a certificate from an OCSP responder. For more information about OCSP, see [“Validating Certificates Using OCSP” on page 289](#).

A dialog box indicates the progress as the certificate is installed on the appliance.

The “Used For” column of the Certificates view indicates the intended use of the certificate.

Figure 97 Certificates view shows installed certificates and their usage

Appliance Name	Subject Name	Used For	Issuer	Expiration	Last Refresh
1cLR	CN=Security Gateway M 00:09:ED:1C...	Management	CN=Security Gateway M 00:...	Tue Nov 20 16:00:4...	Wed Feb 25 15
1c05	CN=Security Gateway M 00:09:ED:00...	Management	CN=Security Gateway M 00:...	Wed Jan 23 09:41:2...	Wed Feb 25 15
2c04	CN=Security Gateway M 00:09:ED:00...	Management	CN=Security Gateway M 00:...	Sun Feb 10 21:29:43...	Wed Feb 25 15

Working with Certificate Requests

The workflow for requesting and installing an identity certificate on an EncrypTight appliance is as follows:

- 1 Generate a certificate signing request.
- 2 Send the request to a CA. If the request is approved, the CA returns a signed certificate.
- 3 Install the signed certificate on the appliance.

Only one certificate request is allowed on the appliance. Prior to creating a new certificate request you must cancel the existing one.

See the following topics to learn about certificate request tasks:

- [“Requesting a Certificate” on page 281](#)
- [“Installing a Signed Certificate” on page 283](#)
- [“Viewing a Pending Certificate Request” on page 283](#)
- [“Canceling a Pending Certificate Request” on page 284](#)
- [“Setting Certificate Request Preferences” on page 284](#)

Requesting a Certificate

Complete the following procedure to create a certificate signing request.

Figure 98 Generate a certificate signing request

To generate a certificate signing request:

- 1 In the Appliances view, right-click the target appliance and click **Generate Certificate Signing Request** in the shortcut menu.
- 2 Complete the Subject Name fields (see [Table 68](#)).
- 3 From the RSA Key Length box, select the size of the key that you want to use. The key is generated using the RSA algorithm. The RSA key size typically refers to the size of the modulus. A larger modulus is more secure, but the algorithm operations are slower. You can select from:
 - 512: Offers little security. Use only for very short-term security needs.
 - 768: Suitable for less valuable information.
 - 1024: Recommended for most corporate use.
 - 2048: Provides the highest level of security.

The Certificate Manager generates a certificate request in Privacy Enhanced Mail (PEM) format.

- 4 When prompted, save the file. The file is saved with a .csr extension.
- 5 Send the certificate request to a certificate authority, following their instructions for completing the request. If the request is successful, the certificate authority will send back an identity certificate that has been digitally signed with the private key of the certificate authority.

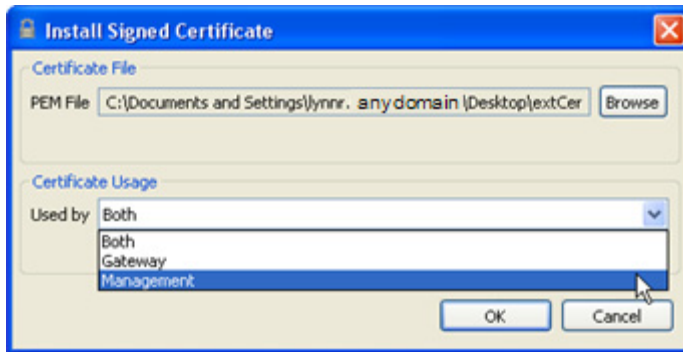
 **NOTE**

ETEMS lets you set default values to be used when generating a certificate request. Many values are common for all certificate requests from a company or division. Setting preferences for these fields can save time when submitting a request. See [“Setting Certificate Request Preferences”](#) on page 284 for more information.

Installing a Signed Certificate

When a certificate authority accepts a certificate request, it issues a digitally signed identity certificate and returns it electronically. The certificate must be a PEM-formatted X.509 certificate. The certificate can be used to validate management communications, data traffic, or both.

Figure 99 Select a certificate file and its usage



To install a signed certificate on an EncrypTight appliance:

- 1 In the Appliances view, right-click the target appliance and click **Install Signed Certificate** in the shortcut menu. The **Install Signed Certificate** window opens.
- 2 In the Certificate File area, click **Browse** to locate the .pem file. Highlight the file and click **Open**.
- 3 In the Certificate Usage area, select which type of data the certificate will authenticate (see [Table 77](#)).
- 4 Click **OK**.

NOTE

*ETEPs that are used as EncrypTight PEPs use certificates only on the management port. **Both** and **Gateway** are invalid options on the ETEP.*

Table 77 Certificate usage

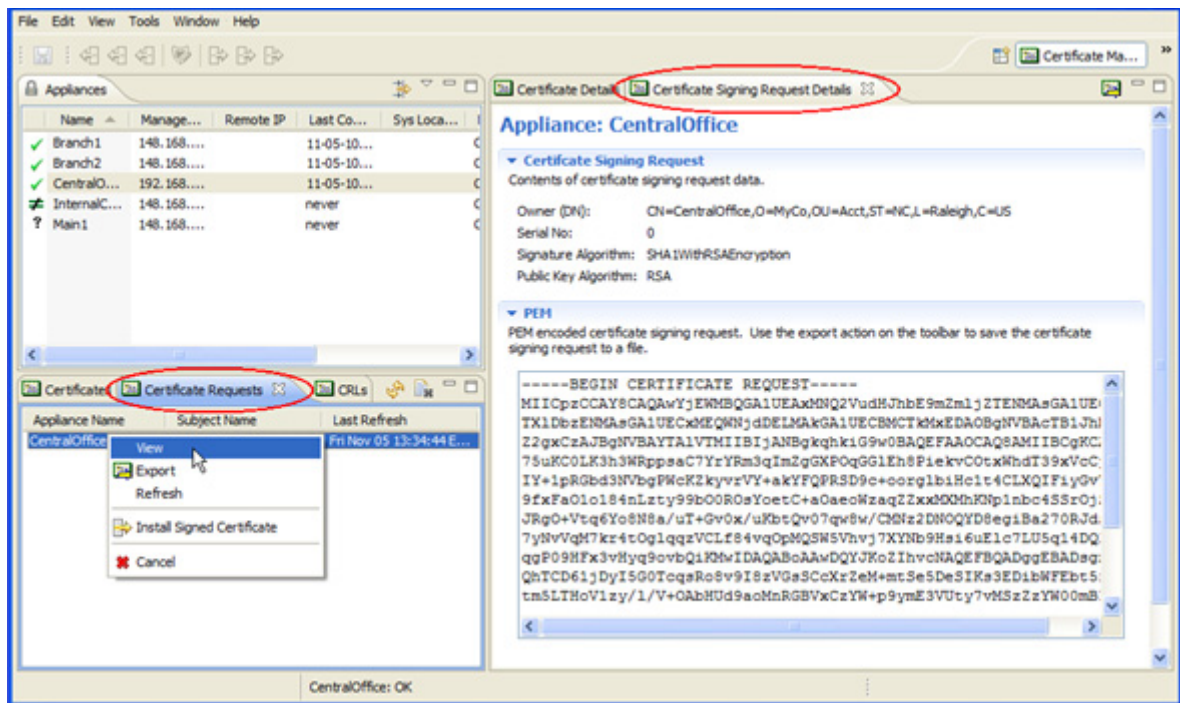
Option	Description
Both	Used for authentication on the management and traffic ports.
Gateway	Used for authentication on the traffic ports.
Management	Used for authentication on the management port.

Viewing a Pending Certificate Request

Pending certificate requests are displayed in the Certificate Request view.

To view a pending certificate signing request:

- 1 In the Appliances view, right-click the target appliance and click **View Certificate Signing Requests** in the shortcut menu. A list of pending certificate requests is displayed in the Certificate Requests view.
- 2 To view the details of a particular request, right-click the target certificate request and click **View** in the shortcut menu. The details of the request display in the Certificate Signing Request Details view.

Figure 100 View pending certificate signing requests

Canceling a Pending Certificate Request

The EncrypTight appliance allows for only one pending certificate request. In order to replace the pending request with a new one, you must cancel the pending request.

To cancel a pending certificate request:

- In the Certificate Request view, right-click the target certificate request and click **Cancel** in the shortcut menu. The pending certificate request is deleted, and you can create a new certificate request.

Setting Certificate Request Preferences

ETEMS lets you set default values that will be used when generating a certificate request. Many values are common for all certificate requests from a company or division. Setting preferences for these fields can save time when generating a request. Any field set in the preferences can be overridden when a certificate request is generated.

To set certificate request preferences:

- 1 Preferences can be accessed from the Appliance manager or the Certificate manager perspective. In the Edit menu, click **Preferences**.
- 2 In the Preferences tree, select **ETEMS > Certificate Manager > Certificate Requests** (see [Figure 101](#)).
- 3 Set the desired default values and click **OK**.

The Common Name (CN) defaults to the appliance name; it cannot be set as a preference. For information about other distinguished name fields, see [Table 68](#). Other certificate requests preferences are described in [Table 78](#).

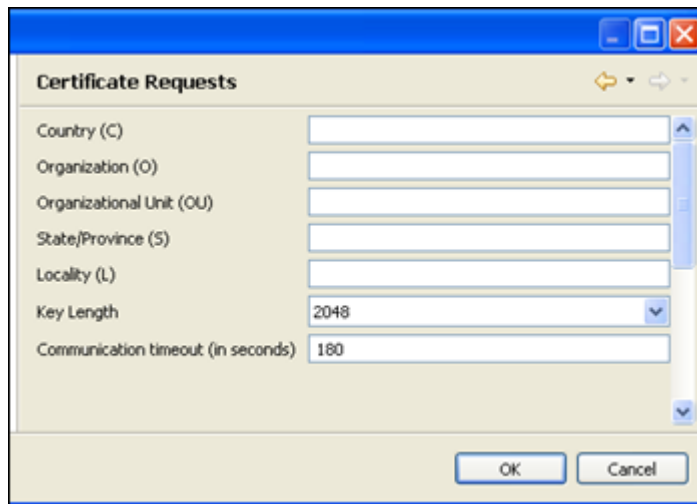
Table 78 Certificate request preference fields

Setting	Description
Key Length	<p>The key is generated using the RSA algorithm. The RSA key size typically refers to the size of the modulus. A larger modulus is more secure, but the algorithm operations are slower.</p> <ul style="list-style-type: none"> • 512: Offers little security. Use only for very short-term security needs. • 768: Suitable for less valuable information. • 1024: Recommended for most corporate use. • 2048: Provides the highest level of security.
Communication timeout	<p>The timeout for generating a certificate signing request. The timeout is specified in seconds. Valid values range from 30 - 300 (5 minutes). The larger the key size, the longer it takes to generate a certificate request.</p>

 **NOTE**

The larger the key size, the longer it takes the EncrypTight appliance to generate the certificate request due to the complexity of the algorithm's operations. A certificate request with a key size of 2048 bits can take several minutes to generate.

Figure 101 Commonly used values can be set as certificate request preferences



Managing Installed Certificates

After certificates are installed on an appliance, you can view them, export them, and delete them. See the following topics to learn more:

- [“Viewing a Certificate” on page 286](#)
- [“Exporting a Certificate” on page 286](#)

- [“Deleting a Certificate” on page 287](#)

Viewing a Certificate


The Certificate Details view of a selected installed certificate displays the certificate contents and the PEM formatted certificate. From the Certificate Details view you can export the certificate using the Export Certificates button  (see [“Exporting a Certificate” on page 286](#)).

Figure 102 Certificate Details view



Exporting a Certificate

This procedure describes how to export an installed certificate from the EncrypTight appliance. The exported certificate can then be installed as a peer certificate on another device.

To export an installed certificate:

- 1 In the Appliances view, right-click the appliance from which to export a certificate, and click **View Certificates** in the shortcut menu. The certificates that are installed on the selected appliance are added to the Certificate view.
- 2 In the Certificates view, right-click the certificate to export and click **Export** in the shortcut menu.
- 3 In the **Save Certificate** window, browse to the location in which to save the file and name the file.
- 4 Click **Save**. The certificate will be saved as a .pem file.

Deleting a Certificate

Delete external certificates if they have expired or are no longer used. External certificates are the only type of certificate that you can delete from the EncrypTight appliance. You can overwrite existing management ID certificates to replace them, but you cannot explicitly delete them.



You must have at least one external certificate installed on the EncrypTight appliance. Deleting an external certificate that is currently being used for authentication will cause management communications to fail.

To delete an external certificate:

- 1 Turn off strict authentication on the ETEP in the configuration editor and push the new configuration, or use the strict client authentication disable CLI command. (For more information, see [“Enabling and Disabling Strict Authentication” on page 292.](#))
- 2 In the Appliances view, right-click the appliance with the certificate that you want to delete, and click **View Certificates** in the shortcut menu. The certificates that are installed on the selected appliance are added to the Certificate view.
- 3 In the Certificates view, right-click the target certificate and click **Delete** from the shortcut menu. The certificate is removed from the Certificates view and is no longer available to authenticate peers.

Validating Certificates

Generally, certificates are considered valid until they expire. However, certificates can be revoked by CAs when necessary. Devices can check the validity of a certificate using certificate revocation lists (CRLs) or the online certificate status protocol (OCSP).

This section includes the following topics:

- [“Validating Certificates Using CRLs” on page 287](#)
- [“Validating Certificates Using OCSP” on page 289](#)

Validating Certificates Using CRLs

Certificate authorities publish certificate revocation lists (CRLs) to identify certificates that it considers invalid. Certificates include a field called a CRL Distribution Point extension, which provides a URL for the certificate authority that has its CRL.

By default, the EncrypTight software and the ETKMSs examine received certificates to determine the URL to use and check this location for CRLs. You must obtain and install a copy of the CRL on the ETEPs that you use.

You can configure the management workstation and the ETKMSs to check for a copy of the CRL in a local directory that you specify. In either case, all EncrypTight components check the CRLs the first time a device initiates communication and then stores the CRL until it expires.

Storing the CRLs locally can accelerate the process of checking CRLs and helps minimize false authentication failures due to revocation check failures. However, if you choose to store CRLs locally,

you must remember to periodically retrieve a copy of the CRL and install it on each of the EncrypTight components.

NOTE

CRLs are only supported in ETEPs with software version 1.6 or later. You must upgrade ETEPs with earlier software versions in order to use this feature. To learn more about upgrading the software on ETEPs, see [“Installing Software Updates” on page 73](#).

Configuring CRL Usage in EncrypTight and the ETKMSs

By default the management workstation and the ETKMS read installed certificates to find the location of the CRL. You can override this behavior and specify a local directory for the CRL instead.

To use CRLs with the EncrypTight software:

- 1 On the management workstation, create a directory where you want to store the CRL files.
- 2 In EncrypTight, select **Edit > Preferences**.
- 3 Click **ETEMS** to expand the tree, and then click **Communications** (see [Figure 95](#)).
- 4 Click **Browse** for the **CRL File Location** option, navigate to the desired directory, and select the CRL.
- 5 Click **Open**.
- 6 Click **OK**.

NOTE

This setting does not take effect until you enable strict authentication.

To use CRLs with the ETKMS:

- 1 Log in as root and create a directory on the ETKMS in which you want to store the CRL.
- 2 Copy the CRL to the new directory on the ETKMS.
- 3 Edit the file `/opt/etkms/conf/kdist.properties` and add the following line in the Certificate Configuration section:

```
crlPath=<Directory>
```

Where <Directory> is the full path to the directory you created.

- 4 Save and close the file.

For example:

```
# Certificate configuration
strictCertificateAuth=true
crlPath=/opt/etkms/crls
```

Configuring CRL Usage on ETEPs

You manage CRLs for the ETEPs using the Certificate Manager perspective in the EncrypTight software.

To install a CRL on the ETEP:

- 1 Switch to the Certificate Manager perspective.
- 2 In the Appliances view, right-click on the target ETEP and choose **Install CRL**.
- 3 Navigate to the appropriate directory and select the CRL file that you want to install.
- 4 Click **Open**.
- 5 Push the modified configuration to the ETEP in order to complete the installation.

To view CRLs

- 1 In the Appliances view, right-click the target ETEP and click **View CRLs** in the shortcut menu. A list of installed CRLs is displayed in the CRLs view.

To delete CRLs

- 1 In the Certificate Manager perspective, select the target ETEP.
- 2 Click the CRLs tab.
- 3 Right-click on the CRL that you want to remove and select **Delete**.

Handling Revocation Check Failures

Not being able to check a CRL does not automatically indicate that a certificate is expired or revoked, especially if the CRL is stored on a server on a different network. By default, if an EncryptTight component cannot check a CRL for any reason, it logs the failure, but still allows a secure communication session to be created. In the EncryptTight software and on the ETKMS, you can change this behavior to fail the authentication instead.

To change the default ETKMS action when a CRL cannot be checked:

- 1 Log in as root and edit the file `/opt/etkms/conf/kdist.properties` and add or edit the following line in the Certificate Configuration section:
`ignoreRevocationCheckErrors=false`
- 2 Save and close the file.

To change the default EncryptTight action when a CRL cannot be checked:

- 1 In EncryptTight, select **Edit > Preferences**.
- 2 Click **ETEMS** to expand the tree and then click **Communications**.
- 3 Click **Ignore CRL access failure** to clear the check box.
- 4 Click **OK**.

Validating Certificates Using OCSP

As an alternative to using CRLs, you can validate certificates with the online certificate status protocol (OCSP). With OCSP, the device that wants to check the validity of a certificate reads the certificate to determine the URL of the OCSP responder and sends a request that identifies the certificate in question. Organizations can also explicitly specify a URL to use for the OCSP responder. The OCSP responder returns a signed OCSP response indicating the validity of the certificate.

In order to use OCSP, you must enable it on each EncrypTight component.

ETEPs can read the URL from the certificate itself, but you can specify a URL to use if needed.

The EncrypTight software and the ETKMSs provide additional options that allow you to specify the default action if no OCSP responder can be located or if the URL cannot be contacted. When OCSP is enabled, EncrypTight and the ETKMS try to check the revocation status using OCSP.

- If no default OCSP responder is defined, then EncrypTight and the ETKMS check the certificate to determine the URL to use to contact an OCSP responder.
- If there is no OCSP URL defined in the certificate, you can specify that EncrypTight and the ETKMS check the certificate for the URL of a CRL Distribution Point as a fallback.
- If the CRL Distribution Point URL is not present or if the URL cannot be reached, the validation fails. Unlike using CRLs only, there is no option to ignore revocation check failures in this scenario.

By default, the system assumes that OCSP responses are signed by the issuer of the certificate whose status is being checked. You can override this and specify an alternative signer by entering the subject name of the signer's certificate.

In addition, in order to verify the response from the OCSP responder, you need to install the certificate from the OCSP responder. For more information about installing certificates, see [“Installing an External Certificate” on page 280](#).

To set up OCSP in EncrypTight:

- 1 In the EncrypTight software, click **Edit > Preferences**.
- 2 In the tree, expand the **ETEMS** item and click **Communications** (see [Figure 95](#)).
- 3 Click **Enable Online Certificate Status Protocol (OCSP)**.
- 4 Configure other options as needed (see [Table 79](#)).
- 5 Click **OK**.

Table 79 EncrypTight OCSP Options

Options	Description
Enable Online Certificate Status Protocol (OCSP)	Enables and disables the use of OCSP in the EncrypTight software. By default, this is disabled.
OCSP Responder Certificate Distinguished Name	Specifies the subject name of the certificate for the OCSP responder.
Verify OCSP Responder	Specifies that messages from the OCSP responder should be authenticated using the installed certificate. To use this option, you must install a certificate for the OCSP responder.
Ignore Failure to Respond	Specifies that the lack of a response from the OCSP responder should be ignored.
Revert to CRL on OCSP Responder Failure	Specifies that if the OCSP responder does not reply or cannot be reached, EncrypTight should read the certificate to determine the location of the CRL to use to validate the certificate. Note that authentication fails when OCSP is enabled and a CRL cannot be accessed as a fallback.
Check OCSP Responder Certificate Chain	Specifies that every certificate in the certificate chain of the OCSP responder should be checked.
OCSP URL	Specifies the URL to use for OCSP checking. This option overrides the use of any OCSP URL that might be indicated in certificates.

 **NOTE**

For enhanced security, if you want to validate certificates using OCSP only, disable the options to **Ignore Failure to Respond** and **Revert to CRL on OCSP Responder Failure**.

To set up OCSP in the ETKMS:

- 1 Log in directly on the ETKMS as root, or open an SSH session and su to root.
- 2 Using a text editor, open the `kdist.properties` file and add or edit the following lines:

```
#crlPath=../keys/current.crl
ocspEnabled=true
ocspDefaultResponderURL=http://<IPaddress:Port#>
ocspCRLFallbackEnable=true
#ignoreRevocationCheckErrors=false
```

Table 80 ETKMS OCSP Parameters

Parameter	Description
<code>crlPath</code>	The directory path to a CRL stored locally. Storing CRLs locally is not supported when you use OCSP. When you use OSCP, this parameter should be commented out by preceding the line with a #.
<code>ocspEnabled</code>	Enables and disables the use of OCSP.
<code>ocspDefaultResponderURL</code>	IP address and port number for a default OCSP responder, for example: <code>http://192.168.42.4:8888</code>
<code>ocspCRLFallbackEnable</code>	Enables and disables checking CRLs if no OCSP default responder is specified and no OCSP URL is found in the certificate, or when a responder cannot be reached.
<code>ignoreRevocationCheckErrors</code>	Specifies whether to ignore revocation check failures for CRLs. When you use OCSP, this parameter should be commented out by preceding the line with a #. Ignoring revocation check failures is not a valid option when OCSP is in use.

To set up OCSP on the ETEPs:

- 1 In the Appliance manager, right click on the appliance that you want to change and select **Configuration**.
- 2 Click the **Advanced** tab.
- 3 Click **Enable OCSP**.
- 4 In the **OCSP URL** box, enter the URL of the OCSP responder.
- 5 Make other selections as needed. See [Table 81](#) for an explanation of the OCSP settings.
- 6 Click **OK**.

Table 81 OCSP Settings

Option	Description
Enable OCSP	When checked, enables the use of OCSP. The default is unchecked.
Verify OCSP Response	Verifies OCSP responses by authenticating the response with the installed certificate. The default is to verify the OCSP response.

Table 81 OCSP Settings

Option	Description
Ignore Failure to Respond	Not receiving a response does not indicate that a certificate has expired or that it has been revoked. This option allows the ETEP to proceed when a response to an OCSP query is not received in a timely manner. The default is to ignore the failure to respond.
Check Certificate Chain	When checked, this option instructs the ETEP to use OCSP to check the validity of every certificate in the responder's chain of trust. The default is unchecked.
OCSP URL	Specifies the URL to use for the OCSP responder.

Enabling and Disabling Strict Authentication

After you have installed certificates on each EncrypTight component, you can enable strict authentication. Strict authentication is a setting that affects communications between all EncrypTight components. Once you enable strict authentication on a component, it begins to use certificates to authenticate communications from devices that attempt to communicate with it. To use strict authentication system-wide, you must specifically enable it in the EncrypTight software, the ETKMSs, and each PEP in use.

To enable strict authentication in the EncrypTight software:

- 1 In EncrypTight, select **Edit > Preferences**.
- 2 Click **ETEMS** to expand the tree, and then click **Communications**.
- 3 Click **Use Strict Certificate Authentication for XML/RPC**.
- 4 Click **OK**.

To enable strict authentication on the ETKMSs, you need to edit the ETKMS properties file. The ETKMS properties file `kdist.properties` is located in the `/opt/etkms/conf` directory.

To enable strict authentication on the ETKMS:

- 1 Log in directly on the ETKMS as root, or open an SSH session and `su` to root.
- 2 Edit the `kdist.properties` file and set the `strictCertificateAuth` property to true. For example:

```
strictCertificateAuth=true
```

- 3 Save and close the file.
- 4 At the command line type

```
service etkms restart
```

To enable strict authentication on PEPs:

- 1 For each PEP, in the Appliance Manager, right-click on the PEP and select **Configuration**.
- 2 In the Configuration editor, click the **Features** tab.
- 3 Click **Enable Strict Client Authentication**.
- 4 Click **OK** to close the warning message.
- 5 Click **OK** to save and close the editor.
- 6 Select all of the PEPs that you changed.
- 7 Click **Put Configuration**.

- 8 Click **Put** to push the configurations.
- 9 Click **Close** to return to the Appliances view, and then refresh the appliance status (**Tools > Refresh Status**).

 **NOTE**

Strict authentication is available for ETEPs with software version 1.6 and later.

If you need to remove the ETEP from service and use it elsewhere, you need to disable strict authentication and remove all certificates and policies.

To disable strict authentication:

- 1 In the Appliance Manager, right-click on the PEP and select **Configuration**.
- 2 In the Configuration editor, click the **Features** tab.
- 3 Clear the **Enable Strict Client Authentication** box.

If certificates expire or if you enable strict authentication before installing certificates, you might not be able to communicate with the ETEP from the management workstation. In this case, you can connect a serial cable to the ETEP and disable strict authentication from the command line.

To disable strict authentication from the command line:

- 1 Connect to the serial port of the appliance and open a terminal session.
- 2 Log in and type **configure** to enter configuration mode.
- 3 Type **management-interface** to enter management interface configuration mode.
- 4 Enter **strict-client-authentication disable**.

For example:

```
admin> configure
Entering configuration mode...
config> management-interface
Entering management interface configuration mode...
man-if> strict-client-authentication disable
```

For more information about using the `strict-client-authentication` command, see the *CLI User Guide* for the ETEP.

Removing Certificates

When you remove all certificates, the appliance regenerates a self-signed certificate. This operation can be performed from the EncrypTight software running on the management workstation, or from a command line window. For information on using the CLI commands, see the *ETEP CLI User Guide*.

To remove certificates:

- 1 If necessary, switch to the Certificate Manager and select the ETEPs whose certificates you want to remove.
- 2 Select **Tools > Clear Certificates**.
- 3 Click **OK** when you are prompted for confirmation.
- 4 Click **OK** at the message informing you that the connection was reset.



Do not use this function if strict authentication is enabled. Doing so can cause errors and prevent communication between the management workstation and the appliance. Disable strict authentication first and then remove the certificates.

Using a Common Access Card

The EncrypTight system supports the use of smart cards such as the DoD Common Access Card (CAC). Using a CAC provides user authorization in addition to certificate-based authentication. When you use a CAC, EncrypTight components use the certificates installed on the card to determine if a user is authorized to perform a specific action. In order to access the system, every user must have an authorized CAC.

A smart card reader is connected to the management workstation. To access the workstation, you must insert a CAC into the reader. The EncrypTight software reads the identity certificate on the CAC, as well as any trusted root or intermediate certificates. When the EncrypTight software communicates with other EncrypTight components, the common name field from the identity certificate is included in the communications. If the common name used in the communications is on the access list, the operation is allowed.

ActivClient must be installed on the management workstation and configured properly for your environment.

Each component in the system must maintain a list of authorized users. Communications that do not use an authorized common name and a valid certificate are rejected.

Setting up the EncrypTight system to use a CAC involves several tasks:

- 1 Install certificates on all EncrypTight components.
This includes the EncrypTight software, the ETKMSs, and the ETEPs. For detailed information and links to the relevant procedures, see [“Using Certificates in an EncrypTight System”](#) on page 265 earlier in this chapter.
- 2 Enable strict authentication on the ETEPs. For more information, see [“Enabling and Disabling Strict Authentication”](#) on page 292.
- 3 Enable Common Access Card Authentication on the ETEPs. For more information, see [“Enabling Common Access Card Authentication”](#) on page 295.
- 4 Add common names to the existing user accounts on the ETEPs, or add new user accounts with common names. You also need to add a user account with a common name for each ETKMS.
For more information, see [“Appliance User Management”](#) on page 102 and [“How EncrypTight Users Work with ETEP Users”](#) on page 67.

- 5 Add the authorized common names to the `cnAuth.cfg` file on the ETKMS. For instructions, see [“Configuring User Accounts for Use With Common Access Cards” on page 295](#)
- 6 Enable strict authentication and Common Access Card Authentication on the ETKMS. For more information, see [“Enabling and Disabling Strict Authentication” on page 292](#) and [“Enabling Common Access Card Authentication” on page 295](#).
- 7 Enable strict authentication and Common Access Card Authentication in the EncrypTight software.

When the EncrypTight software initiates communication with the ETEPs and the ETKMS, it includes the common name read from the identity certificate provided by the CAC.

Configuring User Accounts for Use With Common Access Cards

When Common Access Card Authentication is enabled, you must configure the common name for each EncrypTight user account and for each ETEP user account. The common names also need to be added to the ETKMSs and backup ETKMSs that you use.

The common name field in the user account must match the common name used for the certificate. You can configure this field when you add new users (if Common Access Card Authentication is enabled) or later by editing the user account of an existing user.

For information about working with user accounts, see:

- [“Managing EncrypTight Users” on page 61](#)
- [“Managing Appliance Users” on page 106](#)

User account management on the ETKMS is an operating system function that does not interact with the EncrypTight system. However, you need to add the common names to a list on the ETKMS.

To add common names to the ETKMS:

- 1 Using a text editor, open the file `cnAuth.cfg`, which is located in:
`/opt/etkms/keys`
- 2 Add the authorized common names and save the file. Make sure you include the common names for the certificates used by any peer ETKMSs and backup ETKMSs.

NOTE

You also need to install a copy of the trusted root certificate. For more information, see [“Working with Certificates for EncrypTight and the ETKMSs” on page 272](#).

Enabling Common Access Card Authentication

You must enable Common Access Card Authentication on each ETEP, the ETKMS, and in the EncrypTight software.

To enable CAC Authentication on the ETEP:

- 1 Verify that strict authentication is enabled on the ETEP. If strict authentication is not enabled when you enable Common Access Card Authentication, you can lose the ability to communicate with the ETEP.
- 2 In the Appliance Manager, right-click on the ETEP and select **Configuration** from the shortcut menu.
- 3 Click the **Advanced** tab.
- 4 Click **XML-RPC Certificate Authentication**.
- 5 Click **OK**.
- 6 Push the configuration to the ETEP.

To enable CAC Authentication on the ETKMS:

- 1 Log in directly on the ETKMS as root, or open an SSH session and su to root.
- 2 Edit the `kdist.properties` file and add or edit the following lines:

```
enableCNAuthCheck=true
cnAuthFilePath=../keys/cnAuth.cfg
```
- 3 Save and close the file.
- 4 Repeat steps 1 to 3 on the backup ETKMS.

 **NOTE**

- If you use a backup ETKMS, you also need to add the common name for the certificate used by the backup ETKMS to the list on the primary ETKMS and vice-versa.
- You must also enable strict authentication by including the line `strictCertificateAuth=true`.

To enable CAC Authentication in EncrypTight:

- 1 In the EncrypTight software, choose **Edit > Preferences**.
- 2 In the tree, expand the **ETEMS** item.
- 3 In the tree, click **Login**.
- 4 Click **Enable Common Access Card Authentication**.
- 5 Click **OK**.

When Common Access Card Authentication is enabled, you must insert a valid CAC into the reader before starting the EncrypTight software. When you start the EncrypTight software:

- When you open the EncrypTight software, you are prompted for your EncrypTight user name.
- The software for the reader will prompt you for your PIN.
- If user authentication is enabled, EncrypTight prompts you for your password.
 - If your EncrypTight deployment includes ETEPs running software version 1.6 or later, entering a password is optional.
 - If your deployment includes ETEPs with software previous to 1.6, or other models of PEPs, you must enter a valid password.
- If user authentication is not enabled, you are logged into the system immediately. For more information about working with EncrypTight user accounts, see [“Managing EncrypTight Users” on page 61](#).

 **NOTE**

When Common Access Card Authentication is enabled, users of the EncrypTight software can log in without using passwords if the deployment includes only ETEPs running software version 1.6 or later. However, passwords are still required when administrative users log into the ETEPs using the serial port and through SSH.

Handling Common Name Lookup Failures

When Common Access Card Authentication is enabled, the user accounts for all users who attempt to log into EncrypTight must be configured with common names that match the identity certificate used on their CAC. If the common names do not match or if the user account does not include a common name, by default EncrypTight prompts for a valid user name and password.

If this failsafe mechanism is deactivated, you can be locked out of the system and unable to make changes or troubleshoot the system. However, to provide even greater security you can disable this backup user ID and password prompt.

To specify how to handle common name failures:

- 1 In EncrypTight, choose **Edit > Preferences**.
- 2 Expand the **ETEMS** item and click **Login**.
- 3 Click **On CAC CN Failure, enable User ID/Password authentication** to enable or disable the option.
- 4 Click **Apply** and click **OK**.

21 ETEP Configuration

This chapter provides procedures and reference information for configuring ETEP appliances.

To prepare the ETEP for operation in your network, do the following:

- In the ETEMS Appliance Manager, click **File > New Appliance** to open the Appliance editor. Select the ETEP appliance model from the Product Family list (ET0010A, ET0100A, ET1000A), and select the software version loaded on the ETEP.
- On the Interfaces tab, enter the appliance name.
- On the Interfaces tab, specify the throughput speed at which you want the ETEP to run (ETEP software version 1.6 and later). The throughput speed is determined by the ETEP model and license that you purchased. For more information about throughput speeds and licenses, see [“Managing Licenses” on page 56](#).
- On the Interfaces tab, enter the management port IP address, mask, and gateway.
- On the Features tab, configure the encryption policy setting for Layer 2 or Layer 3. For standalone operation (point-to-point policies), disable EncrypTight.
- Configure the settings appropriate to the type of policies that you will be creating:
 - For distributed key policies, see [“Adding a New PEP in ETEMS” on page 148](#)
 - For point-to-point policies, see [“Creating Layer 2 Point-to-Point Policies” on page 335](#)

You can configure other items as desired, such as auto-negotiation, logging, SNMP trap hosts, or other network interoperability settings. Configuration options vary among software revisions. For a listing of options that are available for each software version and the default settings, see [“Factory Defaults” on page 339](#).

Changing the default password is an important step in maintaining the security of your network. After adding and configuring a new appliance, be sure to add users and passwords prior to pushing the configuration to the appliance. See [“Appliance User Management” on page 102](#) for more information about managing users on ETEP appliances.

If you plan to operate the ETEP in FIPS mode, we recommend enabling FIPS mode as one of your first configuration tasks. Entering FIPS mode resets many configuration items, such as passwords, policies, and certificates. To avoid having to reconfigure the ETEP, enable FIPS mode and then perform the rest of the appliance and policy configuration tasks. See [“FIPS Mode” on page 331](#) for more information about FIPS mode.

This section includes the following topics:

- [Identifying an Appliance](#)
- [Interface Configuration](#)
- [Trusted Hosts](#)
- [SNMP Configuration](#)
- [Logging Configuration](#)
- [Advanced Configuration](#)
- [Features Configuration](#)
- [Working with Policies](#)
- [Factory Defaults](#)

Identifying an Appliance

In order to add an ETEP in ETEMS, you must:

- Specify the product family and software version
- Enter a unique name
- Enter the desired throughput speed (ETEPs with software version 1.6 and later)

The **Interfaces** tab contains the fields that ETEMS uses to identify an appliance and communicate with it: appliance name, throughput speed, management interface IP address, and password (ETEP1.3 only).

Related topics:

- [“Product Family and Software Version” on page 300](#)
- [“Appliance Name” on page 300](#)
- [“Interface Configuration” on page 301](#)
- [“Throughput Speed” on page 301](#)

Product Family and Software Version

When configuring a new appliance (**File > New Appliance**), the first thing to do is select the product family—for example, ET0100A—and the software version loaded on the appliance, such as ETEP1.6. ETEMS displays a configuration screen tailored to the specified appliance model and software version.

Appliance Name

The appliance name is defined on the Interfaces tab. The appliance name identifies an appliance to ETEMS. When the configuration is loaded on the appliance, the appliance name is used as the SNMP system name (MIB2 sysName). Names must adhere to the following conventions:

- Appliance names must be unique
- Names can be 1-255 characters

- Alphanumeric characters are valid (upper and lower case alpha characters and numbers 0-9)
- Spaces are allowed within a name
- The following special characters cannot be used: < > & “ * ? / \ : |
- Names are not case sensitive

Because the appliance name is also the SNMP system name on the appliance, be aware of the following restrictions when copying a name from the appliance to ETEMS. Names with any of the characteristics listed below cannot be copied from an appliance to ETEMS:

- Name with one or more invalid special characters
- Blank name
- Name that is already in use as an appliance name in ETEMS

To learn more about copying configurations from the appliance to ETEMS, see [“Comparing Configurations” on page 100](#).

Throughput Speed

This section applies only to ETEPs with software version 1.6 and later.

In the **Throughput Speed** box, enter the speed at which the ETEP should run. The allowable throughput speed depends on the ETEP model and the license you purchased. ETEMS will only allow you to run the ETEP at the speed for which it is licensed. For more information about licenses and throughput speeds, see [“Managing Licenses” on page 56](#).

Interface Configuration

The ETEP management, local and remote ports are defined on the Interfaces tab ([Figure 103](#)).

To configure appliance interfaces:

- 1 On the **File** menu, click **New Appliance**.
- 2 In the appliance editor, select the product family and software version.
- 3 Configure the items on the **Interfaces** tab, which are described in the rest of this section.
- 4 When you have finished configuring the appliance interfaces, do one of the following:
 - Click one of the other tabs to configure additional parameters.
 - Click **Save and New** to save the appliance configuration and open a New Appliance.
 - Click **Save** to save the appliance configuration.
 - Click **Close** to exit the New Appliance editor.

Figure 103 ET0100A interfaces configuration

The screenshot displays the 'Interfaces' configuration page for an ET0100A appliance. The page is divided into several sections:

- Management Port:**
 - Appliance Name: My new appliance
 - Throughput Speed: 10
 - Use IPv6
 - IPv4:**
 - IP Address: [Empty]
 - Natted IP Address: [Empty]
 - Subnet Mask: 255 . 255 . 255 . 0
 - Default Gateway: [Empty]
 - IPv6:**
 - IPv6 Address: [Empty]
 - IPv6 Default Gateway: [Empty]
 - Auto-negotiate:**
 - Enable
 - Flow Control: On
 - Link Speed: Megabit100FullDuplex
- Transparent Mode:**
 - Transparent Mode
 - Remote Port:**
 - IP Settings:**
 - IP Address: [Empty]
 - Subnet Mask: 255 255 255 0
 - Default Gateway: [Empty]
 - Auto-negotiate:**
 - Enable
 - Flow Control: On
 - Link Speed: Megabit10FullDuplex
 - Transmitter Enable: FollowRx
 - Local Port:**
 - IP Settings:**
 - IP Address: [Empty]
 - Subnet Mask: 255 255 255 0
 - Default Gateway: [Empty]
 - Auto-negotiate:**
 - Enable
 - Flow Control: On
 - Link Speed: Megabit10FullDuplex
 - DHCP Relay IP Address: [Empty]
 - Ignore DFBIT: Enabled
 - Reassembly Mode: Gateway
 - Transmitter Enable: FollowRx

Related topics:

- “Management Port Addressing” on page 302
- “Auto-negotiation - All Ports” on page 305
- “Remote and Local Port Settings” on page 306
- “Transparent Mode” on page 306
- “Trusted Hosts” on page 311

Management Port Addressing

Management of the ETEP is performed out-of-band or in-line through the Ethernet management port. The ETEP management port must have an assigned IP address in order to be managed remotely and communicate with other devices. The IP address that you enter in ETEMS must match the IP address in effect on the appliance’s management port.

ETEPs running software version 1.6 and later include support for IPv4 and IPv6 addresses on the management port.

Related topics:

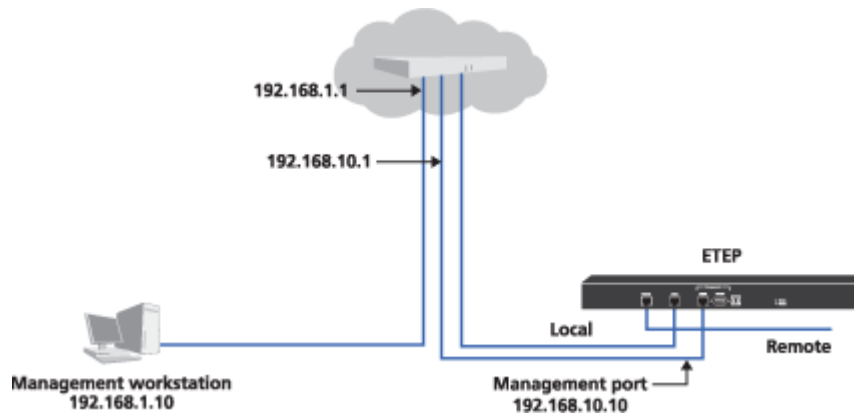
- [“IPv4 Addressing” on page 303](#)
- [“IPv6 Addressing” on page 304](#)

IPv4 Addressing

The ETEP requires an IPv4 address for proper operation, even when it is deployed in an IPv6 network. Enter the IPv4 address, subnet mask, and gateway that is configured on the ETEP’s management port.

Table 82 IPv4 management port addressing

Parameter	Description
IP Address and Subnet Mask	Enter the IPv4 address and subnet mask that has been assigned to the ETEP management port, in dotted decimal notation.
Default Gateway	<p>Specifies how to route traffic between the ETEP management port and the management station and/or EncrypTight ETKMS.</p> <p>When the management port is on a different subnet than the management station or ETKMS, specify the IP address of the router’s local port that is on the same subnet as the ETEP management port. In Figure 104, the default gateway is 192.168.10.1 and the management port IP address is 192.168.10.10.</p> <p>If the other devices are on the same subnet as the management port, you do not need to enter a default gateway.</p>
NAT IP Address	<p>If your network requires the use of allocated IP addresses when communicating over a public network, enter the Network Address Translation (NAT) IP address for ETEMS to use when communicating with the ETEP. If you use a NAT address, you must still configure the management port IP address, subnet mask, and default gateway.</p> <p>The NAT IP address is used only by ETEMS. It is not pushed to the ETEP, therefore it does not appear when comparing the ETEMS and appliance configurations.</p>

Figure 104 Management port default gateway on the EТЕP

IPv6 Addressing

The use of IPv6 addressing is optional. If you select **Use IPv6**, EТЕMS and other EncryрTight components will use IPv6 to communicate with the EТЕP. When using IPv6, you must configure the EТЕP for dual-homed operation by assigning an IPv4 and an IPv6 address to the management port.

To configure the EТЕP for operation in an IPv6 network, do the following:

- 1 Select **Use IPv6**. This tells EncryрTight to use an IPv6 address when communicating with the EТЕP.
- 2 Enter the IPv4 address, subnet mask, and default gateway that is configured on the EТЕP, if you haven't already.
- 3 Enter the IPv6 address and default gateway that is configured on the EТЕP.

Table 83 IPv6 management port addressing

Parameter	Description
IPv6 Address	<p><ip address>/<prefix-length></p> <p>IPv6 address of the EТЕP management port. This is a 128-bit address consisting of eight hexadecimal groups that are separated by colons. Each group is a 4-digit hexadecimal number. The hexadecimal letters in IPv6 addresses are not case sensitive.</p> <p>The prefix length is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address. The decimal value is preceded by a forward slash (/). Valid values are 0-128 inclusive.</p>
IPv6 Default Gateway	IPv6 address of the router port that is on the same local network as the EТЕP management port (see Figure 104).

IPv6 addresses are typically composed of two logical parts: a network prefix (a block of address space, like an IPv4 subnet mask), and a host part. The prefix length indicates the number of bits used for the network portion of the address.

The following is an example of an IPv6 address with a 64-bit prefix:

```
2001:0DB8:0000:0000:0211:11FF:FE58:0743/64
```

IPv6 representation can be simplified by removing the leading zeros in any of the hexadecimal groups. Trailing zeroes may not be removed. Each group must include at least one digit.

IPv6 addresses often contain consecutive groups of zeros. To further simplify address entry, you can use two colons (::) to represent the consecutive groups of zeros when typing the IPv6 address. You can use two colons (::) only once in an IPv6 address.

Table 84 IPv6 address representations

Address Format	Address Representation
Full format	2001:0DB8:0000:0000:0211:11FF:FE58:0743
Leading zeroes dropped	2001:DB8:0:0:211:11FF:FE58:743
Compressed format (two colons) with leading zeroes dropped	2001:DB8::211:11FF:FE58:743

Related topics:

- To learn how to change the management IP address on an appliance after the appliance has been provisioned, see [“Changing the Management IP Address” on page 118](#).
- To learn how to set auto-negotiation on the management port, see [“Auto-negotiation - All Ports” on page 305](#).
- To learn how to restrict access by specifying the hosts that are allowed to communicate with the management port, see [“Trusted Hosts” on page 311](#).

Auto-negotiation - All Ports

Auto-negotiation and flow control are configured on a per port basis. Management, local, and remote port auto-negotiation settings are configured independently of each other. The default setting for the ETEP enables auto-negotiation, which negotiates the link speed, duplex setting, and flow control. If the device to which the ETEP connects from a particular port does not support auto-negotiation or flow control, disable one or both of these functions on that port.

It is essential that the ETEP port and the connecting device’s port are configured the same way. Both devices should either auto-negotiate or be set manually to the same speed and duplex mode. Having one device set manually and the other auto-negotiate can cause problems that make the link perform slowly. When manually setting the ETEP link speed, configure the speed and duplex mode to match that of the other device.

When changing the auto-negotiation setting from ETEMS, there is a slight delay before the new setting takes effect on the ETEP. The delay is typically a few seconds, but can be as long as 30 seconds. During this period, the old setting remains in effect.

On the management port, the ETEPs support the speeds shown in [Table 85](#).

Table 85 Link speeds on the management port

Link speed	Auto-negotiate ET0010A	Auto-negotiate ET0100A / ET1000A	Fixed Speed All ETEPs
10 Mbps Half-duplex	✓	✓	✓
10 Mbps Full-duplex	✓	✓	✓
100 Mbps Half-duplex	✓	✓	✓
100 Mbps Full-duplex	✓	✓	✓
1000 Mbps Full-duplex	✓		

Table 85 Link speeds on the management port

Link speed	Auto-negotiate	Auto-negotiate	Fixed Speed
	ET0010A	ET0100A / ET1000A	All ETEPs
1000 Mbps Half-duplex	✓		

On the local and remote ports, the ETEPs support the speeds shown in [Table 86](#).

Table 86 Link speeds on the local and remote ports

Link speed	Auto-negotiate	Fixed Speed	Fixed Speed
	All ETEPs	ET0010A / ET0100A	ET1000A
10 Mbps Half-duplex	✓	✓	
10 Mbps Full-duplex	✓	✓	
100 Mbps Half-duplex	✓	✓	
100 Mbps Full-duplex	✓	✓	
1000 Mbps Full-duplex	✓		✓

NOTE

If you are using copper SFP transceivers, auto-negotiation must be enabled on the ET1000A and on the device that the ET1000A is connecting to. The recommended copper SFP transceivers negotiate only to 1 Gbps, even though they advertise other speeds. See the ETEP Release Notes for a list of recommended transceivers.

Remote and Local Port Settings

The remote port connects the ETEP to an untrusted network, which is typically a WAN, campus LAN, or MAN. The local port connects the ETEP to a device on the local, trusted side of the network, such as a server or a switch.

See the following topics for configuration details:

- “Auto-negotiation - All Ports” on page 305
- “Transparent Mode” on page 306
- “Local and Remote Port IP Addresses” on page 307
- “Transmitter Enable” on page 308
- “DHCP Relay IP Address” on page 309
- “Ignore DF Bit” on page 310
- “Reassembly Mode” on page 310

Transparent Mode

Transparent mode is the ETEP’s default mode of operation on the local and remote ports. It is appropriate for Layer 2 policies and for most distributed key policies. When operating in transparent mode the ETEP

preserves the network addressing of the protected network by copying the original source IP and MAC addresses from the incoming packet to the outbound packet header.

In transparent mode the ETEP's remote and local ports are not viewable from a network standpoint. The local and remote ports do not use user-assigned IP addresses. In Layer 3 IP networks the local and remote ports cannot be contacted through an IP address, and they do not respond to ARPs. The ETEP is also transparent in Ethernet networks when configured as a Layer 2 encryptor.

If you want to conceal the original source IP address when sending encrypted traffic, configure the ETEP to operate in non-transparent mode. In non-transparent mode, the original source IP address in the outbound packet header is replaced with either an IP address for the remote port or a virtual IP address. The ETEP port MAC address is used as the packet's source MAC address. You must assign IP addresses to the local and remote ports when configuring the ETEP for this mode of operation.

Non-transparency settings apply only when the ETEP is configured for Layer 3 operation and being used in a distributed key policy that uses a virtual IP address or remote IP address.

Table 87 When to use transparent mode

Policy Type	Mode of operation
Layer 2 policies (distributed key mesh and stand-alone point-to-point)	Transparent mode
Layer 3 distributed key policy: Copy the original source IP address to the encryption header	Transparent mode
Layer 3 distributed key policy: Conceal the original source IP address and replace it with one of the following: <ul style="list-style-type: none"> ETEP remote port IP address. This forces traffic through a specific ETEP. User defined virtual IP address. This is useful for load balanced traffic over a private data network, or when sending traffic over the public internet. 	Non-transparent mode

Related topics:

- [“Network Addressing for IP Networks” on page 35](#)
- [“Addressing Mode” on page 185](#)
- [“Local and Remote Port IP Addresses” on page 307](#)
- [“Encryption Policy Settings” on page 334](#)

Local and Remote Port IP Addresses

When transparent mode is disabled, you need to assign an IP address, subnet mask, and default gateway to the local and remote ports. The remote port connects the ETEP to an untrusted network, which is typically a WAN, campus LAN, or MAN. The local port IP address identifies the ETEP to the device on the local side of the network, such as a server or a switch.

 **NOTE**

If you change the remote IP address on an ETEP that is already deployed in a policy, you must redeploy your policies after the new configuration is pushed to the appliance.

IP Address and Subnet Mask

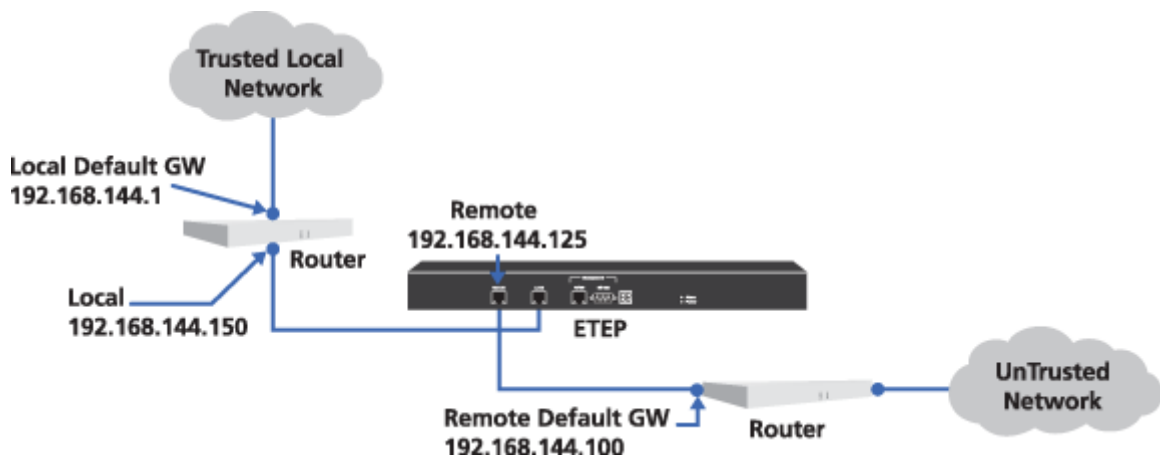
Enter the IP address and subnet mask that you want to assign to the port, in dotted decimal notation.

Default Gateway

The default gateway identifies the router's local access port, which is used to forward packets to their destination. The gateway IP address must be on the same subnet as the port's IP address. In [Figure 105](#), the remote default gateway is the router port 192.168.144.100. The local default gateway address is 192.168.144.1.

A default gateway IP address is required when the ETEP is in a routed network. If the ETEPs are in the same subnet with no routers between them you may leave the default gateway field blank. The ETEP determines if the packet destination is on the same subnet as the port, and if so, uses ARP to resolve the destination MAC address. If the packet destination IP address is on a different subnet, the ETEP sends the packet to the designated default gateway.

Figure 105 Remote port default gateway in a routed network



Related topic:

- [“Transparent Mode” on page 306](#)

Transmitter Enable

The ETEP can be configured to propagate a loss of signal event detected at one of its data ports to the device connected to its other data port. The ETEP performs this function by monitoring for loss of signal at the port's receiver. For example, when the loss of signal is detected on the ETEP's remote port, the local port transmitter is disabled, generating a loss of signal event in connecting device's port. When the loss of signal event clears on the remote port, the local port transmitter is enabled, clearing the event in the connecting device's port. Similarly, when a loss of signal is detected on the local port, the remote port transmitter is disabled.

Alternatively, the ETEP port transmitter can be configured to always remain enabled, regardless of the other port's link state. In this state the ETEP can reliably recover from a link loss. But because the transmitter is always on, the appliance may inadvertently mask cable or device failures in the network.

The transmitter behavior configuration should be the same on both the local and remote ports.

Table 88 Transmitter Enable settings on the ETEP

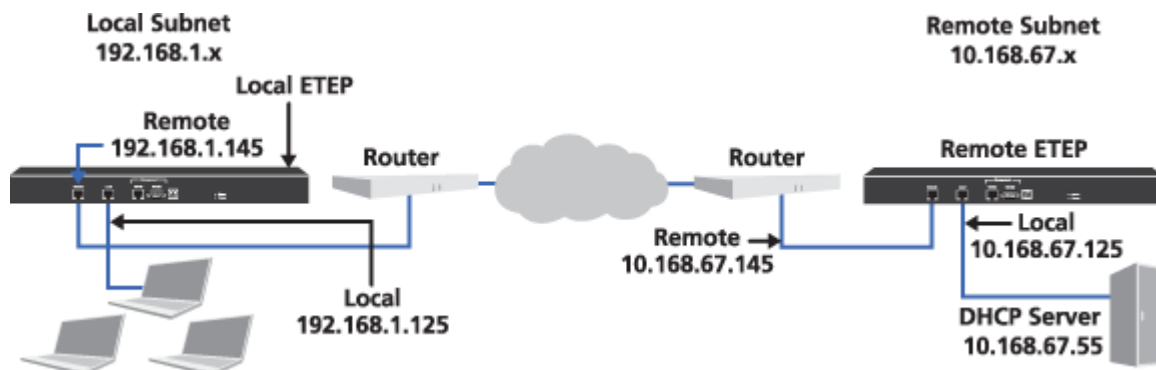
Setting	Description
Follow receiver	The transmitter follows the behavior of the receiver. If loss of signal is detected on the remote port, then the transmitter on the local port is disabled. Similarly, if loss of signal is detected on the local port, the ETEP disables the transmitter on the remote port. When the lost signal is restored, the correlating transmitter is enabled.
Always	The transmitter is always on regardless of whether a signal is received.

DHCP Relay IP Address

The DHCP Relay feature allows DHCP clients on the local port subnet to access a DHCP server that is on a different subnet. The DHCP relay feature is applicable in Layer 3 IP networks.

Enable the DHCP Relay feature only on ETEPs that have DHCP clients on the local port that require access to a DHCP server that is on a different subnet from the local clients (see [Figure 106](#)). This feature is not needed when DHCP servers or relay agents are on the same local network with the DHCP clients, nor is it needed on the ETEP at the remote site where the DHCP server is located.

Figure 106 DHCP Relay allows local clients to access a DHCP server on a remote subnet



Local and remote port IP addresses are required for proper DHCP Relay Agent behavior. In order to use local and remote port IP addresses, the ETEP must be operating in non-transparent mode.

To use the DHCP Relay feature, configure the following items on the Interfaces tab:

- 1 Disable transparent mode.
- 2 Assign local and remote port IP addresses to the ETEP.
- 3 In the **DHCP Relay IP Address** field, enter the IP address of the DHCP server.

Related topics:

- [“Transparent Mode” on page 306](#)
- [“Local and Remote Port IP Addresses” on page 307](#)

Ignore DF Bit

When the ETEP is configured for use in Layer 3 IP encryption policies, its default behavior is to enable DF Bit handling on the local port. This tells the ETEP to ignore the “do not fragment” (DF) bit in the IP header, and fragment outbound packets that exceed the MTU of the system. This setting should be used under the following conditions:

- Reassembly mode is set to **gateway**
- ICMP is blocked at the firewall
- PMTU path discovery isn’t working

A symptom of a PMTU problem is when the network operates normally when traffic passes in the clear but loses packets when encryption is turned on.

You can override the default behavior by disabling the DF Bit handling on the local port. The ETEP will then discard packets in which the DF bit is set and the packet length, including the encryption header, exceed the PMTU.

Table 89 Ignore DF Bit settings

Setting	Description
Enabled	The ETEP ignores the DF bit in the IP header and fragments outbound packets greater than the MTU of the system. This setting is automatically enabled when the reassembly mode is set to gateway .
Disabled	The ETEP acts in accordance with the DF bit setting in the IP header.

Related topic:

- [“Reassembly Mode” on page 310](#)

Reassembly Mode

The reassembly mode setting applies to packets entering the ETEP’s local port that are subject to fragmentation. This setting specifies whether packets are fragmented before or after they are encrypted and who performs the reassembly of the fragmented packet: the destination host or gateway.

The reassembly mode option is available only when the ETEP’s Encryption Policy Setting is set to Layer 3:IP. When the Encryption Policy Setting is set to Layer 2:Ethernet, packets that are subject to fragmentation are encrypted prior to fragmentation. Layer 2 jumbo packets that exceed the PMTU are discarded. The Encryption Policy Setting is configured on the Features tab.

Table 90 Reassembly mode settings

Setting	Description
Gateway	This setting is recommended for ETEP-ETEP encryption. Packets are encrypted first and then fragmented based on the new packet size, which includes the encryption header. This behavior is consistent with RFC 2401. The gateway (ETEP) performs the reassembly. When the reassembly mode is set to gateway, the Ignore DFBit setting is automatically enabled.
Host	This setting is required for the ETEPs to interoperate successfully with some security gateways. Packets are fragmented before they are encrypted, and the encryption header is added to the packet fragments. The destination host performs the reassembly.

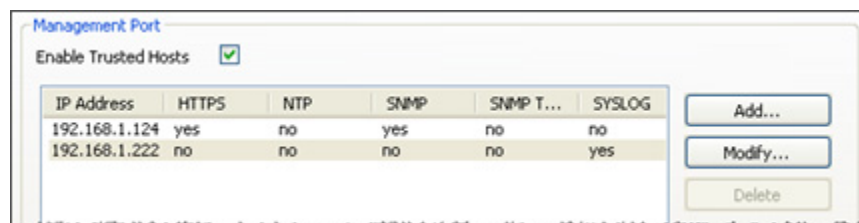
Related topic:

- [“Ignore DF Bit” on page 310](#)
- [“Path Maximum Transmission Unit” on page 326](#)
- [“Features Configuration” on page 330](#)

Trusted Hosts

In its default state the ETEP management port accepts all packets from any host. The trusted host feature lets you restrict access by specifying the hosts that are allowed to communicate with the management port. When the trusted host feature is enabled, packets that are received from non-trusted hosts are discarded. An exception is SSH, which is a secure protocol. It is always allowed regardless of host.

Figure 107 Trusted host list



The ETEMS management station must be included in the trusted host list when the trusted hosts feature is enabled, and at least one trusted host must have HTTPS enabled. HTTPS (TLS) is required for ETEMS to ETEP communications.

If you enter the management station IP address incorrectly, ETEMS will be unable to communicate with the ETEP. To recover, you will need to log in to the CLI and issue the **disable-trusted-hosts** command. See [“Appliance Unreachable” on page 224](#) for more information.

ETKMSs must also be included in the trusted host list. The easiest way to ensure that your ETKMSs are included in the list is to add the ETKMSs in the ETEMS Appliance Manager before enabling the trusted host feature on the ETEP.

If you add a new ETKMS in ETEMS after the trusted host feature is enabled on the ETEP, you can add the ETKMS to its trusted host list in one of the following ways:

- Use the ETKMS in a policy definition in ETPM
- On each ETEP that is using the trusted host feature, clear the **Enable Trusted Hosts** checkbox and then select it again

In either case, you must push the new configuration to the ETEPs for the new trusted host list to become effective. Until you push the new configuration, the ETEP's status is displayed as not equal \neq in the ETEMS Appliance Manager.

The ETEP interacts with two types of hosts:

- Inbound hosts are the management station protocols used to communicate with the ETEP: HTTPS, ICMP, and SNMP.
- Outbound hosts receive packets initiated by the ETEP: SNMP trap hosts, syslog servers, and NTP server hosts.

Inbound host protocols (HTTPS, ICMP, and SNMP) are enabled and disabled in the Edit Trusted Host window. Inbound protocols are enabled by default for each host. Use caution when disabling these protocols as it can affect the management station's ability to communicate with the ETEP.

Table 91 Inbound trusted host protocols used by EncrypTight

Protocol	Description
HTTPS	Used for secure communication between the management station and the ETEP.
ICMP	Used for pings and other diagnostic and routing messages.
SNMP	Used to get SNMP data from the ETEP (name, location, and contact).

You cannot add, modify or delete an *outbound* host directly from the trusted host list. You must make changes in the Appliance editor tab for that feature (Table 92). When you add an outbound host such as a syslog server, NTP server or SNMP trap host to the appliance configuration, the host's IP address is automatically added to the trusted host list. For example, if you add a syslog server in the Appliance editor Logging tab, the syslog server is automatically added to the trusted host list as shown in Figure 107.

The process is similar when deleting an outbound host. Using the syslog server as an example, delete the syslog server from the Logging tab. One of two outcomes occur:

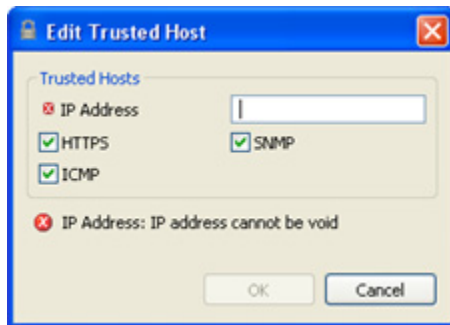
- If no other ports are enabled for that IP address, the trusted host entry is automatically deleted.
- If other ports are enabled for that IP address the change is automatically reflected in the trusted host list, which displays a status of "no" in the Syslog column for that IP address. You can then either leave the modified entry as is, or you can select the trusted host entry and click **Delete** to remove it from the trusted host list.

Table 92 Modify outbound trusted hosts on their respective Appliance editor tabs

Outbound host	Appliance Editor Tab
Syslog server	Logging
NTP	Advanced
SNMP traps	SNMP

To add a trusted host:

- 1 On the Trusted Hosts tab, click **Enable Trusted Hosts**.
- 2 Click **Add**.
- 3 In the Edit Trusted Hosts window, enter the IP address of the trusted host.
With ETEP software version 1.6 and later, you can use either IPv4 or IPv6 addresses.
- 4 Restrict any of the inbound protocols for the host by clearing the checkbox for the protocol (see Table 91). At least one trusted host in the list must have HTTPS enabled.
- 5 Click **OK**. The trusted host and associated protocols appear in the trusted host list.
- 6 Repeat steps 2-5 for each additional trusted host that you want to define.

Figure 108 Trusted host editor**Related topics:**

- [“Appliance Unreachable” on page 224](#)
- [“IPv6 Addressing” on page 304](#)
- [“Traps” on page 315](#)
- [“Defining Syslog Servers” on page 323](#)
- [“SNTP Client Settings” on page 329](#)

SNMP Configuration

The ETEP includes an SNMP agent. When enabled, the SNMP agent in the ETEP sends traps to one or more management stations. Traps can be monitored and viewed using an SNMP network management application.

The ETEP supports SNMPv2c and SNMPv3. You can configure the ETEP to use both types of trap hosts.

Related topics:

- [“System Information” on page 313](#)
- [“Community Strings” on page 314](#)
- [“Traps” on page 315](#)
- [“SNMPv2 Trap Hosts” on page 316](#)
- [“SNMPv3” on page 316](#)

System Information

For managing a number of ETEP appliances from a single management station, it is helpful to have some basic housekeeping information about the SNMP agent in the ETEP, such as its name, location, and a contact person for the device. SNMP uses the Appliance Name as the MIB2 sysName.

Figure 109 SNMP configuration for system information, community strings, and traps

The screenshot shows the SNMP configuration page with the following sections:

- System:** Two text input fields for "Location" and "Contact".
- Community Strings:** A table with columns "Access" and "Value". To the right are buttons for "Add...", "Modify...", and "Delete".
- Traps Generated:** Four checked checkboxes: "Critical Error", "Fan", "Login", and "Generic".

Take note of the following requirements when defining SNMP system information:

- To set the system information on an appliance, the community string must be defined as read/write, as described in [“Community Strings” on page 314](#).
- System information can contain alphanumeric characters and spaces. The following special characters are not allowed: < > “ &

Table 93 SNMP system information

Setting	Definition
Location	Describes the location of the ETEP in the network.
Contact	Defines the designated contact information for the device.

Community Strings

By default the ETEP disregards SNMP requests from a network management station. A community name must be defined for the network management station to monitor and collect statistics from the appliance. The community name identifies a group of devices and management stations running SMNP. An SNMP device or agent can belong to more than one SNMP community. An appliance will not respond to requests from management stations that do not belong to one of its communities.

To define a community name:

- 1 Under **Community Strings**, click **Add**.
- 2 In the **Access** box, select an access option. A read-only community name allows queries of the SNMP agent in the appliance. A read-write community name allows a network management station to perform queries and limited set operations (system location and contact).
- 3 In the **Value** box, enter an SNMP community name. The name is a text string of alphanumeric characters, with a maximum length of 255. All printable characters are valid *except*: < > “ &
- 4 Click **OK**.

Traps

To configure SNMP traps, first select the trap types to be generated. All of the selected trap types will be sent to the configured hosts. Traps cannot be configured on a per-host basis.

Table 94 Traps reported on the ETEP

Trap	Description
Critical error	<p>The following critical errors traps indicate that the ETEP is in an error state:</p> <ul style="list-style-type: none"> criticalFailure: Traffic on the device has been halted and the device is in a failure state. filesystemFailure: Inadequate free space in flash memory. temperatureFailure: The ETEP has exceeded the temperature threshold for safe operation. <p>The following platform warning traps indicate issues that warrant immediate attention, but do not put the ETEP in an error state:</p> <ul style="list-style-type: none"> deployFailure: The ETEP encountered a problem while replacing its policies. certificateManagementWarning: Security certificate management encountered an issue of interest to network operators, such as failed certificate generation, installation, or validation. checkSystemClockWarning: The ETEP detected clock skew that may affect policies. System clock synchronization (NTP) should be checked as soon as possible. filesystemWarning: The filesystem is approaching memory space limits or the syslog daemon is not running. ntpMonitorWarning: The ETEP is unable to synchronize with an NTP server after trying for 30 minutes. powerSupplyWarning: ET1000A only. The ETEP detects problems in one of two redundant power supplies. rekeyFailure: The ETEP encountered a problem while rekeying current policies. temperatureWarning: The operating temperature is approaching unsafe limits. The device should be checked as soon as possible.
Generic	<ul style="list-style-type: none"> coldStart: the SNMP agent has been powered on. notifyShutdown: the SNMP agent is in the process of being shut down. linkUp: one of the communication links has come up (local or remote port). linkDown: one of the communication links has failed (local or remote port). authenticationFailure: the SNMP agent received a packet with an incorrect community string.
Fan	<ul style="list-style-type: none"> fan failed trap down: Fan failure detected. Fan is operating at less than 75% of full speed. fan failed trap up: Fans are operating normally.
Log in	<ul style="list-style-type: none"> Reports successful and failed log in and log out attempts.

 **NOTE**

The `coldStart` and `notifyShutdown` traps are always generated, even when Generic traps are disabled.

Related topics:

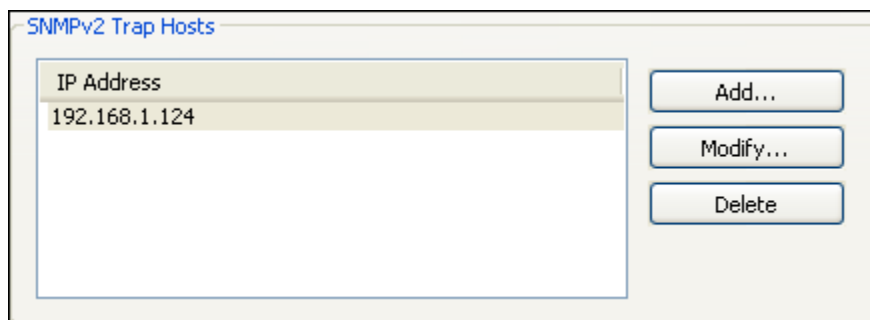
- [“SNMPv2 Trap Hosts” on page 316](#)
- [“SNMPv3” on page 316](#)

SNMPv2 Trap Hosts

After selecting the traps that the ETEP will generate, specify the IP address of the trap hosts that will receive the traps. All of the selected traps are sent to the defined trap hosts. Traps cannot be configured on a per-host basis.

To configure a trap host:

- 1 Under **Trap Hosts**, click **Add**.



- 2 In the **Trap Host** dialog box, enter the trap host’s **IP Address** and then click **OK**. Traps that are enabled on the appliance will be sent to the designated host. Traps are enabled at the appliance level; they cannot be enabled or disabled at the host level.

With ETEP software version 1.6 and later, you can use either IPv4 or IPv6 addresses.

- 3 To finish configuring trap hosts, do one of the following:
 - Click **Add** to add another trap host.
 - Click **Modify** to edit the trap host IP address or traps.
 - Click **Delete** to remove a trap host.

Related topics:

- [“IPv6 Addressing” on page 304](#)
- [“Community Strings” on page 314](#)

SNMPv3

ETEP version 1.6 and later includes support for SNMPv3, in addition to SNMPv2c. You can use either version of SNMP, or both simultaneously.

SNMPv3 enhances security by adding authentication and encryption features.

- The engine ID identifies the ETEP as a unique SNMP entity. The ETEP's engine ID must be configured on every trap recipient before traps can be authenticated and processed by the trap host.
- Three security levels are available to control access to the management information: no authentication and no encryption, authentication and no encryption, and authentication and encryption.
- Trap host users define the destination that receives the traps, plus security information about communication between SNMPv3 entities. Trap host users are defined by a user name, security level, IP address, and optional authentication and encryption parameters. The ETEP supports IPv4 and IPv6 addresses.

In order to exchange messages between an SNMP manager and ETEP agent, both parties have to be configured with the same user. The manager also has to know the ETEP's engine ID. If you want to authenticate communications, the authentication algorithm and authentication key must be known to both parties. For encryption, two more pieces of information are necessary: the encryption algorithm and encryption key. The keys are generated from the authentication and encryption passwords.

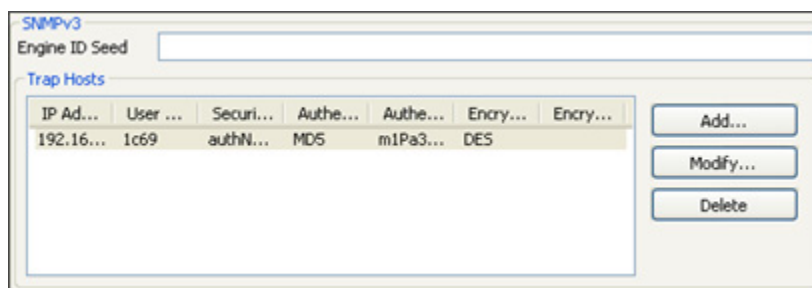
Other notes about the SNMPv3 implementation on the ETEP:

- Traps apply globally to all trap host users. The ETEP does not support trap filtering to individual hosts.
- The ETEP supports SMNPv3 MIB walks when authentication is enabled (security level set to authNoPriv or authPriv).
- To use SNMPv3 with encryption when in FIPS mode, SNMP traffic for each trap host must be secured in an IPsec tunnel.

When using SNMPv3 on the ETEP, do the following:

- 1 Configure the system information and community string.
- 2 Select the traps to enable on the ETEP.
- 3 Select a method for generating the engine ID.
- 4 Configure the SNMPv3 trap host users.

Figure 110 SNMPv3 Configuration



Related topics:

- [“System Information” on page 313](#)
- [“Community Strings” on page 314](#)
- [“Traps” on page 315](#)
- [“Generating the Engine ID” on page 318](#)
- [“Retrieving and Exporting Engine IDs” on page 318](#)

- [“Configuring the SNMPv3 Trap Host Users” on page 319](#)
- [“FIPS Mode” on page 331](#)

Generating the Engine ID

The engine ID is a unique local identifier for the SNMP agent in the ETEP. The ETEP automatically generates its own engine ID upon startup, or you can manually enter an engine ID seed that the ETEP will use to generate the engine ID.

Each ETEP must have a unique engine ID. Duplicate engine IDs can cause SNMP errors. To prevent duplicate IDs, we recommend letting the ETEP generate its own pseudo-random ID. To use the ETEP-generated seed, leave the Engine ID field blank.

If you manually enter an engine ID seed, be sure to use a different seed for each ETEP. Manually entered engine ID seeds must conform to the following conventions:

- The engine ID seed is a string from 1-256 characters.
- Valid values include upper and lower case alpha characters (a-z), numbers 0-9, spaces, and most printable keyboard characters.
- The following characters are not allowed: < > ” &

NOTE

Before the manager can authenticate and process traps generated by the ETEP, you must copy the ETEP's engine ID and trap host user information to the trap hosts.

Related topic:

- [“Retrieving and Exporting Engine IDs” on page 318.](#)

Retrieving and Exporting Engine IDs

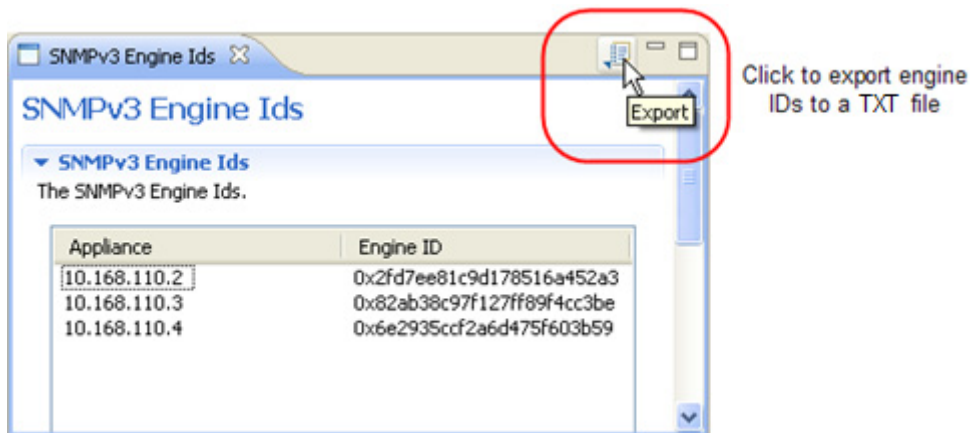
The ETEP's engine ID uniquely identifies the SNMP entity in that ETEP. The ETEP's engine ID must also be configured on every trap host before traps can be authenticated and processed by the trap host.

Using ETEMS, you can retrieve and display the ETEP engine ID. ETEMS can export the engine IDs to a text file. Alternatively, the SNMP engine ID can be viewed from the CLI by issuing the **show running-config** command.

To retrieve engine IDs:

- 1 In the Appliance Manager, select the target appliances in the Appliances view. ETEMS can retrieve the engine IDs from multiple appliances in a single operation.
- 2 On the **View** menu, click **SNMPv3 Engine Ids**. The engine IDs are displayed (see [Figure 111](#)).
- 3 To export the engine IDs to a text file, click the Export button in the upper right corner of the Engine IDs view.
- 4 You will be prompted to save the .TXT file. Browse to a location on the hard drive, enter a filename, and click **Save**.

Figure 111 Viewing SNMPv3 Engine IDs

**Related topics:**

- [“Generating the Engine ID” on page 318](#)

Configuring the SNMPv3 Trap Host Users

Trap host users define the destination that receives the traps, plus security information about communication between SNMPv3 entities. Trap host users are defined by a user name, security level, authentication and encryption parameters, and an IP address. The ETEP supports IPv4 and IPv6 addresses.

 **NOTE**

If you plan to use SNMPv3 with encryption in FIPS mode, SNMP traffic for each trap host must be secured in an IPsec tunnel. See the ETEP CLI User Guide to learn how to create an IPsec policy to secure SNMP traffic on the management port.

Figure 112 SNMPv3 Trap Host configuration
To configure a trap host user:

- 1 If you haven't already done so, select the traps that the ETEP will generate (see [“Traps” on page 315](#)).
- 2 Under SNMPv3 Trap Hosts, click **Add**.
- 3 In the V3 Trap Host dialog box, configure the trap host users as described in [Table 95](#) and then click OK. Traps that are enabled on the appliance will be sent to the designated host. The trap host user information must be configured on both the ETEP and trap recipient.
- 4 To finish configuring trap host users, do one of the following:
 - Click Add to add another trap host.
 - Click Modify to edit the trap host settings.
 - Click Delete to remove a trap host.

Table 95 SNMPv3 trap host users

Field	Description
IP Address	The IP address of the host that will receive the traps generated by the ETEP. With ETEP software version 1.6 and later, you can use either IPv4 or IPv6 addresses.
User name	Name that identifies the ETEP's account to the trap host. The user name / IP address combination must be unique. The user name can be 1-255 characters in length. The following characters are not allowed: < > & " * ? / \ :
Security level	<ul style="list-style-type: none"> • noAuthNoPriv: provides no authentication and no privacy • authNoPriv: provides authentication but no encryption • authPriv: provides authentication and encryption The default is noAuthNoPriv.

Table 95 SNMPv3 trap host users

Field	Description
Authentication Type	SHA. Required for the authNoPriv and authPriv security levels.
Authentication Password	The password is used to generate the authentication key. It is 8-256 characters in length. The following characters are not allowed: ? < > " . ,
Encryption Type	AES. Required with the authPriv security level.
Encryption Password	The password is used to generated the encryption key. It is 8-256 characters in length. The following characters are not allowed: ? < > " . ,

Related topics:

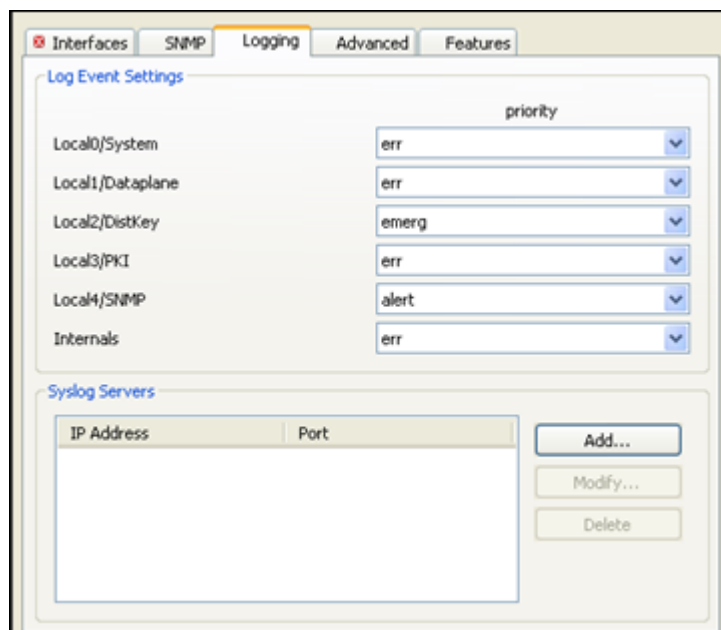
- [“FIPS Mode” on page 331](#)
- *ETEP CLI User Guide*, ‘Securing Management Port Traffic with IPsec’

Logging Configuration

The ETEP log keeps track of messages and events generated by various processes, such as encryption, certificates, rekeys, and SNMP.

All log messages are sent to a log file. You can select the level of information to record by setting the priority for each log facility, which is a category, or grouping, of log messages. Log messages can be viewed in the following ways:

- Configure the ETEP to send log messages to a syslog server
- Use ETEMS to retrieve the log files from an appliance, and view it on the management station as a text file. ETEMS retrieves the log files for each log facility and concatenates them into a single file. It also saves the log files from each facility in separate files.

Figure 113 ETEP Logging tab

Related topics:

- [“Log Event Settings” on page 322](#)
- [“Defining Syslog Servers” on page 323](#)
- [“Log File Management” on page 324](#)
- [“Retrieving Appliance Log Files” on page 228](#)

Log Event Settings

Categories of log messages are referred to as facilities, and they typically indicate which process submitted a message. Each facility can be assigned a priority, which sets the level at which a log message is triggered. Log events settings consist of a log facility and its priority level.

Five facilities are unique to the ETEP. When messages from these facilities are sent to a syslog server, syslog displays their source as Local 0 - Local 4. [Table 96](#) describes each facility and provides a mapping of the ETEP facility name to its syslog counterpart. The Internals facility consists of several operating system facilities.

Table 96 Log facilities

Facility	Description
Local0/System	Significant system events that are not associated with the other pre-defined facilities, including: <ul style="list-style-type: none"> • NTP clock sync successes and failures (informational priority) • Appliance software upgrade status (notice priority) • ET1000A power supply status changes (informational priority) • XML-RPC calls from ETEMS to the ETEP (debug priority)
Local1/Data plane	<ul style="list-style-type: none"> • Messages about packet processing and encryption • PMTU changes (debug priority)
Local 2/DistKey	EncryptTight distributed key functionality, such as rekeys and policy deployments (informational priority)
Local 3/PKI	Certificate messages
Local 4/SNMP	SNMP messages
Internals	Operating system messages for the following Linux facilities: audit, auth and authpriv, cron, daemon, kernel, syslog, user. Audit log events are associated with a user name. The audit log includes events such as the following: <ul style="list-style-type: none"> • Successful and unsuccessful log in attempts • Additions and deletions of ETEP user accounts • Use of administrator functions, such as appliance configuration changes and policy deployments.

The priority determines the amount of information that is recorded for a log facility. When you select a priority for a facility, all messages at that priority and higher are logged; for example a priority of “error”

means “error + critical + alert + emergency.” The priorities shown in [Table 97](#) are listed from lowest (debug) to highest (emergency).

Table 97 Log priorities

Priority	Description
Debug	Detailed processing status. Not recommended during normal operations. The volume of messages may negatively affect the performance of the management port.
Informational	Information messages that do not relate to errors, warnings, audits, or debugging.
Notice	Normal but important events.
Warning	A problem exists, but it doesn't prevent the appliance from completing tasks.
Error	Error conditions and abnormal events.
Critical	Critical condition, for example the appliance is prevented from accomplishing a task.
Alert	Immediate action required. The device will continue to run, but not all functions are available.
Emergency	Emergency; system unusable.

Related topics:

- [“Logging Configuration” on page 321](#)
- [“Defining Syslog Servers” on page 323](#)

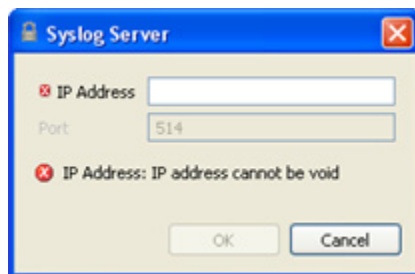
Defining Syslog Servers

The ETEP can send log messages to a syslog server. The ETEP does not impose a limit on the number of syslog servers that can be used. Syslog messages are sent from the management port using port 514 in standard syslog format (RFC 3164). When the facilities are displayed at the syslog server, they appear as Local 0 - Local 4, not as ETEP-specific categories such as data plane, PKI, SNMP, or distkey. See [Table 96](#) for a mapping of log facility names to the numeric syslog designation.

When you configure a syslog server, the messages from all of the facilities are sent to that server, according to the configured priority for each facility. You cannot exclude specific facilities from the list.

To define a syslog server:

- 1 Under **Syslog Servers**, click **Add**.



- 2 In the Syslog Server window, enter the IP address of the syslog server.
With ETEP software version 1.6 and later, you can use either IPv4 or IPv6 addresses.
- 3 Click **OK**.

Related topics:

- [“IPv6 Addressing” on page 304](#)
- [“Logging Configuration” on page 321](#)
- [“Log Event Settings” on page 322](#)

Log File Management

Each log file is a fixed length list of entries, as shown in [Table 98](#). The log files rotate as they fill; they do not wrap. The most recent events are always written to a .log file in the format <logname>.log. When the first log file is full its contents are archived and rotated to logname.log.1.gz. New events continue to be written to the file the .log file. When the logname.log file fills a second time, its contents rotate to logname.log.1.gz and the contents of the previously designated .log.1.gz rotate to .log.2.gz. The log files rotate until five log files have been filled (.log, .log.1.gz, .log.2.gz., .log.3.gz, .log.4.gz). At that point the contents of the oldest log file, .log.4.gz, are deleted.

Table 98 Log file sizes

Log name	File size
audit.log	200k
dataplane.log	250k
distkey.log	250k
pki.log	250k
snmp.log	250k
system.log	500K
Internals logs	
auth.log	100k
cron.log	10k
daemon.log	10k
kern.log	100k
syslog.log	100k
user.log	100k

When ETEMS retrieves the log files from the ETEP, it gets the current and archived log files as individual files. The concatenated file contains only the current log files. Archived log files are saved as compressed .gz files. To view the archived files, use gzip, WinZip, or 7-zip to decompress them.

Figure 114 Log files extracted from the ETEP

Name	Size	Type
audit.log	1 KB	Text Document
auth.log	1 KB	Text Document
authpriv.log	0 KB	Text Document
cron.log	0 KB	Text Document
daemon.log	1 KB	Text Document
dataplane.log	0 KB	Text Document
distkey.log	1 KB	Text Document
kern.log	32 KB	Text Document
pki.log	0 KB	Text Document
snmp.log	5 KB	Text Document
syslog.log	4 KB	Text Document
system.log	426 KB	Text Document
system.log.1.gz	16 KB	WinZip File
system.log.2.gz	16 KB	WinZip File
system.log.3.gz	16 KB	WinZip File
system.log.4.gz	16 KB	WinZip File
user.log	1 KB	Text Document

Related topics:

- [“Retrieving Appliance Log Files” on page 228](#)
- [“Logging Configuration” on page 321](#)
- [“Log Event Settings” on page 322](#)

Advanced Configuration

The items on the Advanced tab define various management and network functions of the appliance, which are described in the following sections:

- [“Path Maximum Transmission Unit” on page 326](#)
- [“Non IP Traffic Handling” on page 327](#)
- [“CLI Inactivity Timer” on page 327](#)
- [“Password Strength Policy” on page 327](#)
- [“XML-RPC Certificate Authentication” on page 328](#)
- [“SSH Access to the ETEP” on page 329](#)
- [“SNTP Client Settings” on page 329](#)
- [“IKE VLAN Tags” on page 329](#)
- [“OCSP Settings” on page 330](#)
- [“Certificate Policy Extensions” on page 330](#)

The settings on the Advanced tab are often the same across appliances, and therefore are good candidates for inclusion in a default configuration as described on [“Working with Default Configurations” on page 110](#).

Path Maximum Transmission Unit

The PMTU specifies the maximum payload size of a packet that can be transmitted by the ETEP. The PMTU value excludes the Ethernet header, which is 14-18 bytes long, and the CRC. The PMTU setting applies to the local and remote ports, as shown in [Table 99](#). On the management port the PMTU is hard-coded to 1400 bytes.

Table 99 Valid PMTU ranges on ETEP appliances

Appliance model	Layer 2 PMTU range	Layer 3 PMTU range	Default
ET0010A	800-1500 bytes	576-1500 bytes	1500
ET0100A // ET1000A	800-9300 bytes	576-9300 bytes	1500

Before sending a packet from its remote or local port the ETEP compares the packet payload size to the configured PMTU. Depending on payload size and appliance configuration the ETEP either discards the packet, transmits the packet, or fragments the packet before transmitting, as described in [Table 100](#).

Table 100 PMTU and fragmentation behavior on the ETEP

Packet Payload Size	Layer 2 ETEP	Layer 3 ETEP
Less than or equal to PMTU	Passes the packet	Passes the packet
Exceeds PMTU	<p>When operating in non-jumbo mode (PMTU \leq1500), the ETEP fragments packets that exceed the PMTU.</p> <p>When operating in jumbo mode (PMTU 1501-9300), the ETEP discards packets that exceed the PMTU.</p>	<p>Fragments the packet if the payload exceeds the PMTU by less than 100 bytes, to allow for encapsulation overhead.</p> <p>Discards the packet under the following circumstances:</p> <ul style="list-style-type: none"> - The payload exceeds the PMTU by more than 100 bytes - The DF bit is set in the IP header.

Fragmentation resolves the problem of encryption overhead, which consists of the extra bytes that are added to the packet as a result of security encapsulation. For example, a packet with a payload size of 1500 bytes may pass through the network without being discarded. But after encapsulation, the payload size increases by 37-52 bytes. The resulting larger packet may be rejected by some equipment located in the network between the two peer appliances. By fragmenting the packet, the separate fragments are not rejected by the network.

The ETEP can be configured to perform pre-encryption or post-encryption fragmentation when it is operating as a Layer 3 encryptor. This feature is called Reassembly mode, and it is defined on the Interfaces tab in the Appliance editor. Reassembly mode cannot be configured when the Encryption Policy Setting is set to Layer 2:Ethernet. At Layer 2, packets that are subject to fragmentation are encrypted prior to fragmentation. Jumbo packets that exceed the PMTU are discarded.

When the ETEP is configured as a Layer 3 encryptor, the ETEP discards packets that exceed the PMTU size and have the DF (do not fragment) bit set in the IP header. You can override the DF bit in the IP header using the Ignore DF Bit setting on the local port.

Related topics:

- [“Ignore DF Bit” on page 310](#)

- [“Reassembly Mode” on page 310](#)
- [“Features Configuration” on page 330](#)

Non IP Traffic Handling

The non IP traffic handling setting is available when the ETEP is configured for use in Layer 3 encryption policies. This setting provides options for how to handle Layer 2 packets that are not IP at Layer 3. Non-IP packets can be discarded or passed in the clear. When discarding non-IP traffic, you have the option of passing ARP packets in the clear or discarding them as well. All packets that are IP at Layer 3 are handled according to the policies that are loaded on the appliance.

When the non-IP discard feature is enabled, the appliance looks at the packet’s Layer 3 protocol flag. If the protocol flag is IP, then the appliance processes the packet normally. If the protocol flag is non-IP, then the appliance discards the packet. This processing applies to both inbound and outbound packets.

The appliance’s default setting is **clear**, where non-IP packets are passed in the clear and IP packets are processed according to the policies loaded on the appliance.

Table 101 Non IP traffic handling configuration

Setting	Description
clear	All packets that are non-IP at Layer 3 are passed in the clear.
discard	All packets that are non-IP at Layer 3 are discarded. ARP packets are excluded from the discard action.
discardIncludingARP	All packets that are non-IP at Layer 3 are discarded, including ARP packets.

Related topic:

- [“Features Configuration” on page 330](#)

CLI Inactivity Timer

The CLI session is terminated if no activity is detected on the CLI in a specified amount of time. The inactivity timer is set to 10 minutes by default. The timer applies to a CLI session initiated through the serial port or through SSH.

The inactivity timer is specified in minutes, with valid values ranging from 0–1440 minutes (24 hours). When the CLI inactivity timer is set to zero the session does not time out.

Setting the inactivity timer does not affect the current CLI session. The change is effective on all subsequent CLI sessions.

Password Strength Policy

The password strength policy affects the following items:

- Password conventions
- Password history exclusion, which limits the reuse of passwords
- Password expirations, warnings, and grace periods

- Maximum number of concurrent login sessions allowed per user
- The number of login failures allowed before locking an account

The strong password policy enforces more stringent password rules and conventions than the default password policy. The default password policy is enforced unless you explicitly enable the strong password policy.

 **NOTE**

Enabling strong password enforcement restarts the SSH daemon, closing any open SSH connections between ETEMS and the ETEP. It can take up to 30 seconds to re-establish an SSH connection after enabling strong passwords.

Related topics:

- [“Default Password Policy Conventions” on page 104](#)
- [“Strong Password Policy Conventions” on page 104](#)

XML-RPC Certificate Authentication

The remote user certificate authentication on the ETEP is required to support the Common Access Card (smart card) feature in an EncrypTight deployment.

The EncrypTight system supports the use of smart cards such as the DoD Common Access Card (CAC). The use of a CAC provides user authorization in addition to certificate-based authentication. When you use CACs, EncrypTight components use the certificates installed on the card to determine if a user is authorized to perform a specific action.

Setting up the ETEP to use a CAC involves several tasks:

- 1 Install certificates on the ETEPs. This task is performed using the EncrypTight software.
- 2 Enable strict authentication on the ETEPs.
- 3 Enable Common Access Card Authentication on the ETEPs
- 4 Add common names to the existing user accounts on the ETEPs, or add new user accounts with common names. These names must match the common names used on the identity certificates included on the CACs.

Additional steps are required to prepare the EncrypTight workstation and ETKMS to use strict authentication with smart cards. Be sure to complete all of the required steps in order, as described in [“Using Enhanced Security Features” on page 261](#).

Related topics:

- [“Adding ETEP Users” on page 106](#)
- [“Using a Common Access Card” on page 294](#)
- [“EncrypTight Settings” on page 333](#)

SSH Access to the ETEP

SSH is used for secure remote CLI management sessions through the Ethernet management port. SSH access to the appliance is enabled by default.

To prevent remote access to the CLI, clear the **Enable SSH** checkbox. When SSH is disabled, CLI access is limited to the serial port.

Related topic:

- [“Connecting to the Command Line Interface” on page 123](#)

SNTP Client Settings

The ETEP includes a Network Time Protocol (NTP) client, which is used to synchronize the appliance time with an NTP server. NTP is useful in minimizing or eliminating clock drift that can occur over time, and keeping timestamps of log events consistent across appliances and other devices in the network.

The NTP client supports unicast client mode, in which the client (ETEP) sends a request to a designated NTP server and waits for a reply from the server. The ETEP synchronizes with the NTP service at a dynamic interval inherent in the operating system's NTP client.

Time synchronization with the NTP time service overrides any manually set date and time. The UTC offset is unaffected.

To configure the NTP client:

- 1 Click the **Enable SNTP Client** checkbox.
- 2 Enter the IP address of the NTP service.

With ETEP software version 1.6 and later, you can use either IPv4 or IPv6 addresses.

Related topic:

- [“Changing Settings on Multiple Appliances” on page 121](#)
- [“IPv6 Addressing” on page 304](#)

IKE VLAN Tags

When the ETEP is configured for operation with Layer 2 point-to-point policies, the two ETEPs must be able to communicate with each other to exchange key information. In some Layer 2 networks, all frames must have a VLAN tag to traverse the network. The ETEP can be configured to add a VLAN tag to the Ethernet frames used for ETEP-to-ETEP communications.

This setting has no effect when the ETEP is configured for use in EncrypTight distributed key policies.

The following settings are prerequisites for configuring this feature:

- 1 On the Features tab, set the Encryption Policy Setting to **Layer 2:Ethernet**.
- 2 On the Features tab, clear the **Enable EncrypTight** checkbox.

- 3 On the Advanced tab, select **Enable IKE VLAN Tag**.

Table 102 IKE VLAN Tags

Field	Description
IKE VLAN tag priority	Sets the VLAN priority. Valid values range from 0-7.
IKE VLAN tag identifier	Sets the VLAN ID. Valid values range from 0-4094.

OCSP Settings

Online Certificate Status Protocol (OCSP) provides a way for devices that use certificates to verify that a received certificate is currently valid. OCSP is an alternative to using Certificate Revocation Lists (CRLs). If your organization uses certificates to authenticate management communications in an EncrypTight deployment, you can use OCSP to check the validity of the certificates you install.

Related topics:

- [“Using Enhanced Security Features” on page 261](#)
- [“Validating Certificates Using OCSP” on page 289](#)

Certificate Policy Extensions

Certificate policy extensions indicate the purposes for which a certificate was issued, for example signing e-mail or encryption. If your organization uses certificates and makes use of the certificate policy extension, you can enable support for the extensions on the EТЕP and enter the allowable OIDs.

Related topics:

- [“Using Enhanced Security Features” on page 261](#)
- [“Configuring the Certificate Policies Extension” on page 269,](#)

Features Configuration

The items on the Features tab define what kind of policies the EТЕP can enforce and what layer of traffic it acts on.

- [“FIPS Mode” on page 331](#)
Configures the EТЕP for FIPS mode operation (supported in specific versions of EТЕP software).
- [“EncrypTight Settings” on page 333](#)
Determines whether the EТЕP will enforce EncrypTight distributed key policies or stand-alone point-to-point policies. Also enables strict authentication on the EТЕP.
- [“Encryption Policy Settings” on page 334](#)
Configures the EТЕP for use in Layer 2 or Layer 3 policies.

FIPS Mode

When operating in FIPS mode, the ETEP must be configured to use FIPS-approved encryption and authentication algorithms. FIPS approved algorithms are listed in [Table 103](#). Note that some of the FIPS-approved algorithms are available for use only on the management port.

EncrypTight prevents the ETEP from entering FIPS mode if ETPM detects EncrypTight distributed key policies that contain non-FIPS approved algorithms.

The ETEP prevents entry into FIPS mode when any of the following conditions are true:

- EncrypTight distributed key policies are installed that use non-FIPS approved algorithms
- IKE policies are configured on the management port interface that use non-FIPS approved algorithms
- Manual key policies are installed on the management port interface. If you plan to use manual key policies, deploy them after FIPS mode is enabled on the ETEP.
- SNMPv3 configuration uses cryptography for SNMP trap hosts, but no IPsec policy has been configured to protect the SNMP traffic for each specific trap host
- The debug shell is in use
- Strict client authentication is enabled on the management port

If you plan to use strict authentication to secure management port communications, you must enable FIPS mode prior to enabling strict authentication. To learn more about using strict authentication, see the [“About Strict Authentication” on page 262](#) and [“Order of Operations” on page 263](#).

Table 103 FIPS approved encryption and authentication algorithms

Encryption algorithms	Authentication algorithms
3des-cbc	sha1-96-hmac
aes128-cbc	sha2-256-hmac
aes256-cbc	sha2-384-hmac

Related topics:

- [“About Strict Authentication” on page 262](#)
- [“Order of Operations” on page 263](#)
- [“SNMPv3” on page 316](#)
- *ETEP CLI User Guide*, “FIPS 140-2 Level 2 Operation”

Enabling FIPS Mode

To configure the ETEP for FIPS operation, select the **Enable FIPS Mode** checkbox.

After pushing a FIPS-enabled configuration to the ETEP, it takes several minutes for the ETEP to enter FIPS mode. Some communications services are reset when FIPS is enabled and disabled. SSH sessions are terminated, and cannot be reestablished until FIPS mode is fully operational. You may experience a brief loss of connectivity between the ETEP and ETEMS.

When putting the ETEP in FIPS mode, the ETEP performs the following actions and self-tests:

- Runs self-tests during the boot process and when entering FIPS mode that include cryptographic algorithm tests, firmware integrity tests, and critical function tests

- Performs a software integrity test
- Clears pre-existing policies and keys, as described in [Table 104](#).
- Generates a new self-signed certificate on the management interface
- Removes all externally signed certificates
- Resets passwords to the factory defaults
- Closes remote SSH client sessions

Table 104 Effects of clearing policies and keys when entering FIPS mode

Policy Type	Action upon entering FIPS mode
Distributed key policies	Traffic passes in the clear until new encryption policies are created and deployed to the EТЕP.
Point-to-point Layer 2 policies	Keys are automatically renegotiated. Traffic is discarded in the interim.
Management port policies	Keys are automatically renegotiated. Traffic is discarded in the interim.

Operational Notes

Entering FIPS mode may cause some delays when communicating with the EТЕP.

- When the EТЕP is rebooted with FIPS mode enabled, the EТЕP does not become operational until 30-60 seconds after the login prompt is displayed. In the interim, attempts to communicate with the EТЕP from EТЕMS or the CLI result in error messages (attempting to access a locked shared resource or failure to create input stream). If you receive an error message, wait several seconds and retry.
- The Ethernet management interface uses FIPS-approved cipher and authentication algorithms for SSL and SSH connections. When operating in FIPS mode, it can take 30-60 seconds to establish an SSH session.
- If you used SSH to manage the EТЕP prior to entering FIPS mode, you may not be able to establish an SSH session after FIPS is enabled. To correct this, clear the known host entry for your SSH client and retry.

Disabling FIPS

The EТЕP performs the following actions when exiting FIPS mode:

- Existing policies continue to run until they are replaced or deleted.
- SSH is reset when FIPS is disabled, terminating the current session.

Verifying FIPS Status on the EТЕP

You can verify that FIPS is enabled on the EТЕP in the following two ways:

- In EТЕMS, compare the EТЕMS and EТЕP configurations (**Tools > Compare Config to Appliance**).
- Log in to the CLI and issue one of the following commands: **show running-config** or **show fips-mode**.

Related topics:

- [“Connecting Directly to an Appliance” on page 123](#)

- [“EncryptTight Settings” on page 333](#)
- [“Encryption Policy Settings” on page 334](#)
- [“Creating Layer 2 Point-to-Point Policies” on page 335](#)
- *ETEP CLI User Guide*, “FIPS 140-2 Level 2 Operation”

EncryptTight Settings

The EncryptTight settings define whether the ETEP is to be used as a PEP in an EncryptTight system or operate as a standalone point-to-point encryptor.

- To configure Layer 2 or Layer 3 distributed key policies, select the **Enable EncryptTight** checkbox. Select the encryption policy setting for Layer 2:Ethernet or Layer 3:IP policies. Use EncryptTight ETPM to create and deploy distributed key policies.
- To configure Layer 2 point-to-point policies, select the **Layer 2:Ethernet** encryption policy setting and clear the **Enable EncryptTight** checkbox. Use the Policy tab in ETEMS to configure Layer 2 point-to-point policies.

Table 105 EncryptTight settings

Setting	Definition
Enable EncryptTight	<ul style="list-style-type: none"> • Select this option to use the ETEP as a policy enforcement point (PEP) in an EncryptTight distributed key deployment. • Clear the checkbox to use the ETEP in a Layer 2 point-to-point policy.
Pass TLS traffic in the clear	<p>Passing TLS-based management traffic in the clear is required for EncryptTight distributed key policies, and when the ETEP is managed in-line. When the ETEP is operating in Layer 2 distributed key mode, ARP traffic is also passed in the clear when <code>tls-clear</code> is set to true.</p> <p>This option is unavailable when the EncryptTight feature is disabled.</p>
Enable strict client authentication	<p>EncryptTight uses TLS to encrypt traffic between EncryptTight components. EncryptTight can use TLS with encryption only, or TLS with encryption and strict authentication. When strict authentication is enabled, TLS enforces certificate-based authentication among the EncryptTight components (ETPM, ETKMSs, and PEPs). See “Using Enhanced Security Features” on page 261 for procedures to install certificates and enable strict authentication on the various components of the EncryptTight system.</p>



CAUTION

Certificates must be installed on the ETEP prior to pushing a configuration that enables strict client authentication. Enabling strict authentication without first installing certificates locks up the ETEP’s management port.

Related topics:

- [“About Strict Authentication” on page 262](#)
- [“Using Certificates in an EncryptTight System” on page 265](#)
- [“Enabling and Disabling Strict Authentication” on page 292](#)

- [“Encryption Policy Settings” on page 334](#)
- [“Working with Policies” on page 334](#)

Encryption Policy Settings

The Encryption Policy Setting determines the type of policies that the Etep can be used in: Layer 2 Ethernet policies or Layer 3 IP policies. Appliances that are configured for Layer 2 cannot be used in Layer 3 policies, and vice versa. If you intend to create a Layer 4 policy to encrypt only the packet payload, set the Encryption Policy Setting to Layer 3:IP.

Table 106 Encryption policy settings

Setting	Definition
Layer 2: Ethernet	Enable this setting to use the Etep in Layer 2 Ethernet policies. Point-to-point policies are defined in ETEMS; mesh policies are defined in EncrypTight ETPM.
Layer 3: IP	Enable this setting to use the Etep in Layer 3 IP policies, or if you intend to create a policy to encrypt only the Layer 4 payload. Layer 3 distributed key policies are defined in EncrypTight ETPM.

When you change the encryption policy setting of an in-service Etep, all encrypt and drop policies currently installed on the Etep are removed and all traffic is sent in the clear until you create and deploy new policies, or until the policies are rekeyed. A rekey installs an “encrypt all” policy on the Etep.

If you are using EncrypTight, take the following steps to ensure proper enforcement of your distributed key policies when you change the encryption policy setting:

- 1 In the ETEMS Features tab, change the Encryption Policy Setting to Layer 2 or Layer 3.
- 2 Push the new configuration to the Etep (**Tools > Put Configuration**).
- 3 In ETPM, delete the policy that contains the original Etep configuration.
- 4 Create a new policy for the reconfigured Etep.
- 5 Deploy the new policy.

Related topics:

- [“EncrypTight Settings” on page 333](#)
- [“Working with Policies” on page 334](#)

Working with Policies

ETEMS’s primary function is configuring and managing appliances from a central workstation. After you have configured the ETEPs for network operation, you have the following options for creating and deploying policies:

- EncrypTight distributed key policies (mesh, hub and spoke, multicast, Layer 3 point-to-point) are created and managed using ETPM.
- Layer 2 point-to-point policies are created using the policy editor in the ETEMS Policy tab.

Related topics:

- [“Using EncrypTight Distributed Key Policies” on page 335](#)
- [“Creating Layer 2 Point-to-Point Policies” on page 335](#)


Using EncrypTight Distributed Key Policies

After you have configured the ETEPs for network operation, use the Policy Manager (ETPM) to create and deploy distributed key policies.

ETPM can create Layer 2 mesh policies and the following types of Layer 3 policies:

- Mesh
- Hub and spoke
- Multicast
- Point-to-point

To launch ETPM from ETEMS:

- 1 Do one of the following from any EncrypTight perspective:
 - In the Window menu, click **Open**. Click **Other**. In the Open Perspective window, select ETPM and click **OK**.
 - On the Perspective tab in the upper right corner of the screen, click the Open Perspective button . Click **Other**. In the Open Perspective window, select ETPM and click **OK**.

Related topics:

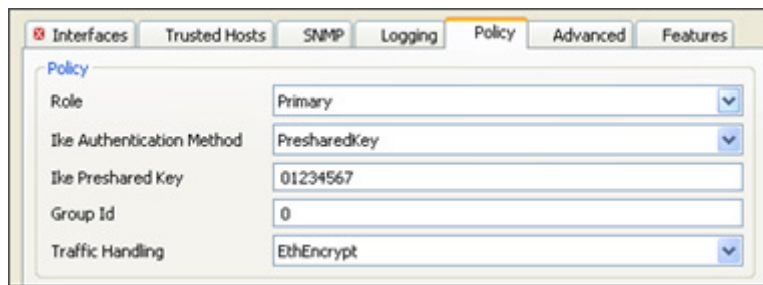
- [“Getting Started with ETPM” on page 131](#)
- [“Creating Distributed Key Policies” on page 181](#)
- [“Creating Layer 2 Point-to-Point Policies” on page 335](#)

Creating Layer 2 Point-to-Point Policies

Layer 2 point-to-point policies are created using the policy editor in the ETEMS Policy tab. The following settings are prerequisites for using this feature:

- 1 On the Features tab, set the Encryption Policy Setting to **Layer 2:Ethernet**.
- 2 On the Features tab, clear the **Enable EncrypTight** checkbox.

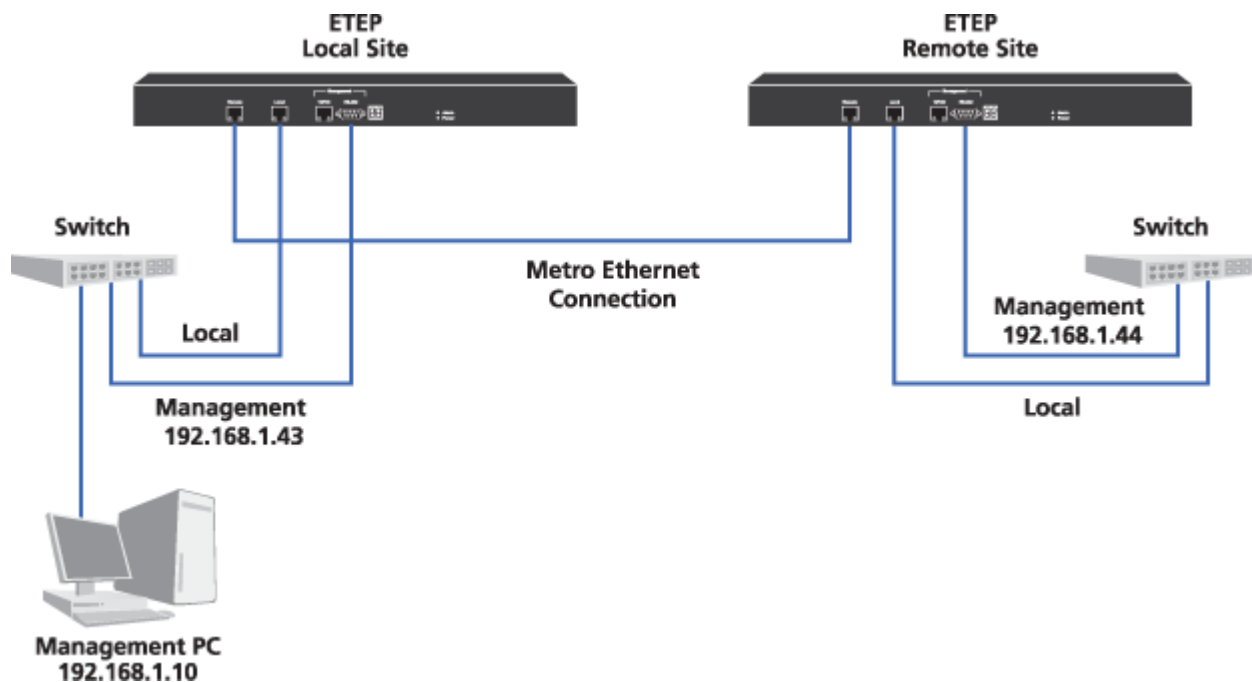
On the Policy tab, just a few settings are needed to configure the ETEP to encrypt traffic. The policies on the two ETEPs must use the identical preshared key and group ID, and be assigned *opposite* roles (primary and secondary). As with any other appliance configuration setting, you have to push the policy to the ETEPs for it to take effect.

Figure 115 ETEP Policy tab


Policy	
Role	Primary
IKE Authentication Method	PresharedKey
IKE Preshared Key	01234567
Group Id	0
Traffic Handling	EthEncrypt

When ETEPs are first installed they pass all traffic in the clear until they receive policies. After you push the Layer 2 point-to-point policy configuration to the ETEPs they will begin negotiations to encrypt traffic. You can change the way in which the ETEP processes traffic by modifying the traffic handling setting to pass traffic in the clear, discard traffic, or encrypt traffic.

If you are managing the ETEPs in-line as shown in [Figure 116](#), the order in which you push configurations to the ETEPs is important. The local ETEP (#2 in [Figure 116](#)) must be passing traffic in the clear in order to push a configuration to the remote ETEP (#3 [Figure 116](#)). To maintain connectivity with the remote ETEP's management port, push the configuration to the remote ETEP first and then push the configuration to the local ETEP.

Figure 116 Point-to-point Layer 2 Ethernet link

Note the following operational constraints and recommendations:

- Layer 2 point-to-point IKE policies are incompatible with local site manual key policies that are created from the command line.
- When the ETEP is configured for Layer 2 point-to-point operation, the management port IKE server is shut down, which prevents IKE SAs from being negotiated on the management port. If you plan to

deploy management port IPsec policies while in Layer 2 point-to-point mode, use manual key policies to encrypt management port traffic.

- We recommend setting the time on the ETEPs before setting up the Layer 2 point-to-point policy. Changing the clocks after the policy is established may cause traffic to be dropped.

Related topics:

- [“Selecting a Role” on page 337](#)
- [“Using Preshared Keys for IKE Authentication” on page 337](#)
- [“Using Group IDs” on page 337](#)
- [“Selecting the Traffic Handling Mode” on page 338](#)
- [“EncryptTight Settings” on page 333](#)
- [“Encryption Policy Settings” on page 334](#)
- [“How the ETEP Encrypts and Authenticates Traffic” on page 338](#)

Selecting a Role

The appliance role is used in the process of establishing a security association (SA) between ETEP peers. The ETEP can assume one of two appliance roles when it is configured for point-to-point operation. One of the appliances must be assigned the primary role and the other the secondary role. The ETEPs will not function properly if both appliances are configured with the same role.

Using Preshared Keys for IKE Authentication

In point-to-point Layer 2 networks, the ETEPs use IKE negotiations to establish security associations (SAs) between peer appliances. The ETEP uses the preshared key string to authenticate its peer’s identity before the ETEPs begin to negotiate the SAs. *The same key value must be entered in both appliances.*

We recommend that you change the key from its default value of 01234567 prior to deploying the ETEP. Note the following conventions when creating a preshared key:

- The key is a case-sensitive alphanumeric string from 8-255 characters in length
- Valid characters are upper and lower alpha characters, numbers 0-9
- All special characters are allowed *except* the following: ? “ { } [] () = \ < > & and #
- To include a space, enclose it in double quotes.

Using Group IDs

In a point-to-point network, the two ETEPs must be configured with the same group ID in order to communicate properly with each other. If you are using only one pair of ETEPs in the same subnet you can use the default group ID.

If more than one pair of ETEPs is used within the same Layer 2 network, the group ID isolates the traffic from one pair of ETEPs from any other pair. Each appliance can belong to only one group.

Selecting the Traffic Handling Mode

The ETEP has three options for processing packets:

- Encrypt all packets
- Discard all packets
- Pass all packets in the clear

Under normal operation, the ETEP is configured to encrypt all traffic that is exchanged between two peer appliances. This is the ETEP's default mode of operation. Other methods of traffic handling are used for debugging and troubleshooting. The traffic handling setting persists through a reboot.

How the ETEP Encrypts and Authenticates Traffic

When operating as a Layer 2 encryptor in a point-to-point policy, the ETEP's encapsulation mode authenticates the encrypted frame's Ethernet payload. The ETEP uses the AES algorithm with 256-bit keys to encrypt the Ethernet payload. The HMAC-SHA-1 authentication algorithm provides the data origin authentication and data integrity.

Figure 117 Layer 2 encrypted frame format



To encrypt traffic, ETEPs must establish *security associations* (SAs). A security association defines the processing to be done on a specific packet. It associates security services and a key with the traffic to be protected and the remote peer with whom secured traffic is being exchanged. The SA is a unidirectional secure tunnel through which data passes between the two appliances. Each secure connection has two SAs, one for each direction. SAs are identified by a value called an SPI.

In point-to-point Layer 2 configurations the SAs are automatically negotiated using IKE. Timeout values force the IKE protocol to renegotiate the IKE Phase 1 and Phase 2 keys periodically. The ETEP can use a preshared key for authentication in IKE negotiations.

When encrypting traffic the ETEP uses the values shown in [Table 107](#) and [Table 108](#). These values are hard-coded and cannot be modified by the user.

Table 107 IKE Phase 1 Parameters

Parameter	Value
Cipher algorithm	AES-256
Hash algorithm	HMAC-SHA-1
Diffie-Hellman group	5
Lifetime	24 hours
Negotiation mode	Main mode

Table 108 IKE Phase 2 Parameters

Parameter	Value
Cipher algorithm	AES-256

Table 108 IKE Phase 2 Parameters

Parameter	Value
Hash algorithm	HMAC-SHA-1
PFS Diffie-Hellman group	5
Lifetime	One hour
Negotiation mode	Main mode

Factory Defaults

ETEMS's factory settings are listed by appliance model and software version for the following categories:

- [Interfaces](#)
- [Trusted Hosts](#)
- [SNMP](#)
- [Logging](#)
- [Policy](#)
- [Advanced](#)
- [Features](#)
- [Hard-coded Settings](#)

Interfaces

Table 109 Interfaces defaults

Interfaces	Default Setting
Appliance Identification	
Remote user password	Not applicable
Appliance name	model number_version (e.g., ET0100A_ETEP1.6)
Throughput speed	Undefined
Management	
IPv4 address	Undefined
Subnet mask	255.255.255.0
IPv4 default gateway	None
Natted IP address	Undefined
IPv6 address	Undefined
IPv6 default gateway	Undefined
Flow control	Negotiated
Link speed	Negotiated
Remote	
Transparent mode	Enabled
IP address	Undefined
Subnet mask	255.255.255.0

Table 109 Interfaces defaults

Interfaces	Default Setting
Default gateway	None
Flow control	Negotiated
Link speed	Negotiated
Transmitter enable	FollowRx
Local	
IP address	Undefined
Subnet mask	255.255.255.0
Default gateway	None
Flow control	Negotiated
Link speed	Negotiated
DHCP Relay IP Address	Undefined
Ignore DF Bit	Enabled
Reassembly mode	Gateway
Transmitter enable	FollowRx

Trusted Hosts

Table 110 Trusted hosts defaults

Trusted Hosts	Default Setting
Enabled trusted hosts	Disabled

SNMP

Table 111 SNMP defaults

SNMP	Default Setting
Contact	Undefined
Location	Undefined
Community string	Undefined
Traps	
Critical error trap	Enabled
Fan trap	Enabled
Generic trap	Enabled
Login	Enabled
Trap Hosts	
SNMPv2 trap hosts	Undefined
SNMPv3 trap hosts	Undefined

Logging

Table 112 Logging defaults

Logging	Default Setting
Local 0 / System	Informational
Local 1 / Dataplane	Informational
Local 2 / DistKey	Informational
Local 3 / PKI	Informational
Local 4 / SNMP	Informational
Internal	Informational
Syslog server	None

Policy

Table 113 Policy defaults

Policy	Default Setting
Role	Primary
IKE Authentication	Preshared key
IKE Preshared Key	01234567
Group ID	0
Traffic Handling	EthEncrypt

Advanced

Table 114 Advanced defaults

Advanced	Default Setting
PMTU	1500
Non IP traffic handling	Clear
CLI Inactivity Timer	10 minutes
Password Policy	Disabled
XML-RPC Certificate Authentication	Disabled
SSH Enable	Enabled
SNTP Client	None
IKE VLAN tag	Disabled
OCSP Settings	Disabled
Certificate Policy Extensions	Disabled

Features

Table 115 Features defaults

Features	Default Setting
Enable FIPS Mode	Not available
Enable EncrypTight	Enabled (user configurable)
Enable TLS in the clear	Enabled
Encryption Policy Settings	Layer 3:IP
Enable strict client authentication	Disabled

Hard-coded Settings

The following settings are hard-coded in the ETEP:

- Management port PMTU is 1400 bytes
- Syslog server port is 514
- Time zone is set to UTC 0

Index

Numerics

3DES, 184

A

addressing mode, 171, 185
advanced configuration
 ETEP, 325–329
Advanced Encryption Standard, 184
AES, 184
appliance configuration
 customizing default configurations, 110
 EETP, 299–342
 importing from a CSV file, 112
 overview, 95
 restoring factory defaults, 111
appliance users *See* user accounts
appliance-level tasks
 connecting to the CLI, 123
 managing ETEP user accounts, 106
 retrieving log files, 228
appliances
 adding a new appliance, 96, 147
 deleting, 122
 editing a configuration, 117
 filtering by management IP address, 101
 selecting a group of appliances, 88
 shutting down, 116
 status, viewing, 98
appliances view, 88
application log
 deleting, 236
 exporting, 235
 filtering, 235
 restoring, 236
 sending events to a syslog server, 235
 viewing, 234
apply to all traffic, minimizing mesh policy size,
 187
ARIA encryption, 184
authentication

algorithms, 184
auto-negotiation configuration
 EETP, 305

B

backing up
 appliance file system, 123
 workspace, 70
backup ETKMSs, 29
banner, displaying at login, 64
bypass mode, passing clear traffic for
 troubleshooting, 246
bypass policy action, 138

C

CAC, 294
canceling a software upgrade, 127
Certificate Manager
 cancelling a pending certificate request, 284
 certificate request preferences, setting, 284
 CRLs
 deleting from ETEPs, 289
 installing on ETEPs, 288
 viewing on ETEPs, 289
 deleting external certificates, 287
 exporting certificates, 286
 generating certificate requests, 281
 installing a signed certificate, 283
 installing external certificates, 280
 obtaining external certificates, 279
 overview, 278
 starting, 277
 toolbar, 90
 viewing installed certificates, 286
 viewing pending certificate requests, 283
 workflow, 279
certificate policy extensions, 269
 configuring in EncrypTight, 270
 configuring on a ETKMS, 270
 configuring on ETEPs, 269

- certificate revocation lists (CRLs), see CRLs, 287
- certificates
 - See also Certificate Manager
 - about, 262
 - and common access cards, 294
 - certificate policy extensions, 269
 - certificate revocation lists (CRLs), 287
 - configuring CRL usage, 287
 - configuring CRL usage in EncrypTight, 288
 - configuring CRL usage on the ETKMS, 288
 - deleting all on an ETEP, 293
 - deleting specific certificates from an ETEP, 287
 - distinguished name, 264
 - EncrypTight keystore password, 266
 - errors, 249
 - ETKMS keystore password, 266
 - exporting from EncrypTight or the ETKMS, 275
 - generating a key pair, 272
 - generating a key pair (EncrypTight and the ETKMS), 273
 - handling revocation check failures, 289
 - HSM, 275
 - HSM keystore password, 268
 - importing CA certificates for EncrypTight and the ETKMS, 274
 - importing certificate replies for EncrypTight and the ETKMS, 274
 - invalid, 250
 - keytool, 272
 - OCSF configuration, 289
 - planning for the use of, 34
 - policy constraint extension, 271
 - policy ETPMping, 271
 - prerequisites, 263
 - recommended order of operations, 263
 - requesting for EncrypTight and the ETKMS, 273
 - strict authentication, 262
 - disabling, 293
 - enabling, 292
 - using in an EncrypTight system, 265
- chkconfig --list | fgrep "3 on" command, 242
- chkconfig --list command, 242
- CLI inactivity timer
 - ETEP, 327
- clock synchronization using SNTP
 - ETEP, 329
 - overview for EncrypTight components, 33
- command line interface (CLI)
 - connecting to the CLI from ETEMS, 123
 - diagnostic commands, accessing, 233
- commands
 - chkconfig --list, 242
 - chkconfig --list | fgrep "3 on", 242
 - service --status-all, 242
 - service --status-all | fgrep "is running", 242
- common access card (CAC), 256, 294, 328
 - common name, 294
- common name, 294
- Communication preferences, 92
- communication timeout, changing, 92
- comparing
 - configurations, 100
- configuration for CipherEngine
 - KAP network connection, 49
- configuration for EncrypTight
 - ETKMS admin password, 47
 - ETKMS date and time properties, 51
 - ETKMS root password, 48
 - external ETKMS, 46
 - local ETKMS, 44
 - PEP, 55, 148
- configurations on appliances
 - comparing, 100
 - defining default configurations, 110
 - deleting, 122
 - downloading to appliances, 97
 - editing, 117
 - pushing, 97, 151
 - saving, 97
- configuring an appliance
 - ETEP, 299–342
 - overview, 95
- connections
 - ETKMS to PEP, 31
 - ETPM and local ETKMS to PEP, 26
 - ETPM to ETKMS, 26
 - external ETKMS to ETKMS, 29
- copying a workspace to a new PC, 72
- copying an appliance configuration to ETEMS, 100
- counters, viewing, 230
- CRLs
 - about, 287
 - communication preferences, 94
 - configuring usage in EncrypTight, 288
 - configuring usage on a ETKMS, 288
 - deleting from ETEPs, 289
 - installing on ETEP, 288
 - viewing on ETEPs, 289
- CSV files, importing appliance configurations, 112
- CSV files, importing PEP configurations, 150
- customer support, 14
- customized default configurations, 150

D

- database
 - See workspace
- date and time
 - about clock synchronization, 33
 - changing on an appliance, 121
 - configuring on the ETKMS, 51
- default configurations, 110
 - modifying defaults, 110
 - restoring, 121
 - using factory settings, 111
- default ETKMS, 185
- default gateway configuration
 - ETEP management port, 302
 - ETEP remote and local ports, 308
- default user accounts and passwords, 56
- deleting
 - appliances, 122
 - policies, 209
 - workspace, 72
- deploy policies
 - procedure, 207
 - receiving confirmation, 208
 - status icon, 137
- deployment planning for EncryptTight, 25–??
- DES, 184
- DF bit configuration
 - ETEP, 310
- DHCP Relay, configuring on the ETEP, 309
- diagnostic tools
 - See *also* troubleshooting
 - CLI commands, 233
 - exporting SAD and SPD files, 232
 - viewing discarded packet status, 232
 - viewing port status, 232
 - viewing statistics, 230
- dialog boxes
 - Change Date, 121
 - Edit Appliance, 121
 - Edit Default Configuration, 110
 - Preferences, 92
 - Put Configurations, 97
 - Upgrade Appliances, 123
- discarded packet status, viewing, 232
- distinguished name, 264
- distributed key policies, supported topologies, 17
- downloading
 - appliance configurations, 97
 - software upgrades, 123
- drop policy action, 138

E

- Edit menu commands
 - Change Keystore Password, 266
 - Change User Password, 66
 - Configuration, 117
 - Date, 121
 - Default Configurations, 110
 - Delete, 122
 - Management Address, 118
 - Multiple Configurations, 121
 - Preferences
 - Certificate Manager, 284
 - Communications, 92
 - Login, 62
 - ping tool, 228
 - Tools, 227
 - User Accounts, 65
- editing
 - date and time, 121
 - default configurations, 110
 - ETKMSs, 157
 - management IP address, 118
 - multiple appliance configurations, 121
 - date and time, 120
 - using a CSV import file, 115
 - network set, 174
 - networks, 164
 - PEPs, 151
 - policies, 209
 - single appliance configuration, 121
 - VLAN ID range, 179
- editors
 - ETEMS, 88
 - ETPM, 134
- enabling EncryptTight on a PEP, 149
- encapsulation method used in EncryptTight, 183
- encrypt all policies with exETEPTions, defining, 185
- EncryptTight
 - components view, 133
 - configuring on the ETEP, 330
 - exiting the application, 41
 - license, 56
 - starting the application, 40
- encryption
 - algorithms in EncryptTight, 184
 - changing from Layer 3 to Layer 2, 334
 - policy settings
 - changing on the ETEP, 334
 - statistics, 245
- error log See application log
- ETEMS overview
 - comparing configurations, 85

- defining appliance configurations, 83
 - maintenance and troubleshooting, 86
 - policy and certificate support, 87
 - pushing configurations, 84
 - upgrading software, 85
 - ETEP
 - license, 56
 - replacing license, 245
 - throughput, 301
 - ETEP configuration, 299–342
 - Ethernet policies at Layer 2, adding, 188
 - ETKMS
 - configuration
 - changing the admin password, 47
 - changing the root password, 48
 - checking the status of the ETKMS service, 53, 54
 - configuring the time and date properties, 51
 - external ETKMS overview, 46
 - external ETKMS, installing hardware, 43
 - external ETKMS, logging in, 47
 - HSM, 256
 - local ETKMS IP address, 44
 - local ETKMS overview, 44
 - local ETKMS, launching, 45
 - local ETKMS, starting automatically, 45
 - local ETKMS, stopping, 45
 - securing the server with the front bezel, 54
 - connections
 - backup ETKMSs, 29
 - ETKMS to PEP connections, 31
 - ETPM and local ETKMS to PEP, 26
 - ETPM to ETKMS, different subnetworks, 27
 - ETPM to ETKMS, same subnetwork, 27
 - external ETKMS to ETKMS connections, 29
 - key storage, 24
 - management
 - modifying the ETKMS properties file, 255
 - overview, 20
 - start the ETKMS service, 53
 - status, 54
 - stop the ETKMS service, 53
 - troubleshooting
 - log files, 241
 - rebooting an external ETKMS, 243
 - recovering the admin account, 243
 - restarting the ETKMS, 243
 - server operation, 242
 - shutting down an external ETKMS, 243
 - using with ETPM
 - adding ETKMSs, 156
 - assigning an appliance name, 157
 - default ETKMS, 185
 - deleting a ETKMS, 157
 - editing ETKMSs, 157
 - global ETKMS, 185
 - setting the management port IP address, 157
 - using a backup ETKMS, 156
 - ETKMS keystore password, 266
 - ETPM
 - creating a policy, overview, 141
 - deployment warning, 208
 - enabling automatic status checking, 137
 - launching, 131
 - menu bar functions, 135
 - policies description, 138
 - Ethernet policies, 138
 - IP policies, 138
 - policy generation and distribution, 139
 - policy view, 135
 - status indicators, 135
 - user interface overview, 131
 - using ETPM editors, 134
 - ETPM to ETKMS connections, 26
 - exiting EncryptTight, 41
 - exporting
 - appliance log files, 228
 - certificates from the appliance, 286
 - SAD and SPD files, 232
 - external certificates
 - See also* Certificate Manager
 - deleting, 287
 - installing, 280
 - obtaining, 279
 - viewing, 286
- ## F
- factory settings
 - defaults
 - ETEP, 339–342
 - restoring, 111
 - features
 - configuring on the ETEP, 330
 - File menu commands
 - Close, close all, 97
 - Load Workspace, 71
 - New Appliance, 95
 - Save Workspace To, 70
 - Save, save all, 97
 - filtering
 - filtering appliances by address in ETEMS, 101
 - filtering criteria in policies, 138
 - FIPS mode, enabling on the ETEP, 331

firewall ports, 39
 flow control configuration
 ETEP, 305
 fragmentation
 ETEP
 choosing the reassembly mode, 310
 setting the PMTU, 326
 FTP server
 configuring for software upgrades, 125
 enabling on the management station, 42

G

global ETKMS, 185
 group ID
 ETEP, 337
 grouping networks, 161

H

hardware requirements, 38
 hardware security module
 See also HSM
 HTTPS (TLS), 42
 hub and spoke policy, adding, 191

I

ignore DF bit
 ETEP, 310
 ignore source IP address, 187
 IKE
 Phase 1 parameters, 338
 Phase 2 parameters, 338
 IKE VLAN tag, enabling, 329
 importing appliance configurations from a CSV file
 changing import preferences, 115
 creating an import file, 112, 150
 importing remote and local interface addresses, 114
 importing ETPM configurations from a CSV file, 172
 inactivity timer
 EncrypTight session, 63
 EETP, 327
 in-band management
 See in-line management
 in-line management
 appliance upgrade considerations, 75, 124
 configure PEPs to pass TLS traffic in the clear, 26
 installation
 appliance software upgrades, 123

ETKMS hardware, 43
 firewall ports, 39
 hardware requirements for management station, 38
 installing EncrypTight for the first time, 39
 software updates, 73
 third party software requirements, 38
 uninstalling EncrypTight software, 40
 upgrading to a new version of EncrypTight, 40
 interface configuration
 EETP, 301–310
 invalid certificate, 250
 invalid parameter, 250
 IP network addressing, specifying the source IP address in the encapsulated packet header, 35
 IPSec (encrypt) as a policy action, 138
 IPv6
 EncrypTight support for, 33

K

KAP
 adding backup KAPs, 50
 configuration
 configuring the network connection, 49
 key generation and distribution, 139
 Key Management System, *see* ETKMS
 key storage
 See also keystore
 keystore
 EncrypTight keystore password, 266
 ETKMS keystore password, 266
 HSM keystore password, 268
 keytool
 See also certificates
 generating a key pair, 272
 importing CA certificates, 274
 importing certificate replies, 274
 requesting certificates, 273

L

last comm attempt, ETEMS appliances view, 100
 Layer 2
 adding a new mesh policy, 188
 adding a point-to-point policy, 335
 out-of-band management, 25
 point-to-point policy example, 211
 using a VLAN policy for management traffic, 25
 Layer 4
 adding a new Layer 4 policy, 206
 encapsulation method, 183

- hub and spoke policy addressing mode
 - override, 193
- mesh policy addressing mode override, 197
- multicast policy addressing mode override, 201
- payload encryption policy, 185
- point-to-point policy addressing mode
 - override, 205
- license, 56
 - EncryptTight, 57
 - ETEP, 57
 - replacing ETEPs, 245
 - upgrading, 58
- link speed configuration
 - ETEP, 305
- Linux commands for external ETKMSs, 242
- load balancing, 35
- loading
 - configurations, 97
 - software updates, 125
 - workspaces, 71
- local port configuration
 - ETEP, 306–308
- log files
 - application log for EncryptTight, 234
 - ETKMS, 241
 - ETPM, 241
 - PEP, 242
 - retrieving appliance log files, 228
- logging configuration
 - ETEP, 321–325
- login banner, enabling for EncryptTight, 64
- login preferences for EncryptTight, 62

M

- management port
 - configuration
 - auto-negotiation, 305
 - ETEP, 302
 - NAT, 303
 - IP address, changing, 118
 - options for securing communications, 42
- management station
 - FTP server configuration, 42
 - securing the management interface, 42
 - syslog server configuration, 43
 - third party software, 38
- MD5, 184
- mesh policy, adding, 195
- Message Digest #5, 184
- metapolicy, 139
- Microsoft FTP server configuration, 42
- minimize policy size, 187

- multicast policy, adding, 199
- multiple configurations, editing, 121

N

- naming the appliance
 - ETEP, 301
- NAT on the ETEP management port, configuring, 303
- negotiated key topology, 22
- negotiated point-to-point policy, 22, 335
- network
 - adding, 159
 - addressing methods, 35
 - deleting, 164
 - grouping into supernets, 161
 - importing from a CSV file, 172
 - IP address, 160
 - mask, 160
 - modifying, 164
 - preserving IP addresses, 35
 - transparent mode, 35
 - using non-contiguous network masks, 162
- network clocks, synchronizing, 33
- network connections, configuring the KAP interface, 49
- network interfaces, PEP settings, 148
- network logs, viewing, 228
- network masks, non-contiguous, 162
- network set, 167
 - adding, 170
 - addressing mode, 185
 - default ETKMS, 171
 - deleting, 174
 - importing from a CSV file, 172
 - modifying, 174
 - types, 168
- Network Time Protocol (NTP), using for EncryptTight clock synchronization, 33
- network topology
 - for distributed key policies
 - hub and spoke, 18
 - mesh, 18
 - multicast, 18
 - point to point, 18
 - for negotiated policies, 22
- new appliance, configuring, *See* appliance configuration
- non-contiguous network masks, using in network sets, 162
- non-IP traffic handling, configuring on the ETEP, 327
- non-transparent mode
 - see* virtual IP address

NTP, 149

O

OCSP

- about, 289
- communication preferences, 94
- enabling in EncryptTight, 290
- enabling in ETEPs, 291
- enabling on ETKMSs, 291

open perspective, 131

out-of-band management

- ETKMS to ETKMS connections, 30
- ETKMS to PEP connections, 32
- ETPM to ETKMS connections, 28

P

passing TLS traffic in the clear, 149

password

- changing the ETKMS admin password, 47
- changing the ETKMS root password, 48
- configuring the ETEP password strength policy, 327
- default password conventions on the ETEP, 104
- default passwords for EncryptTight components, 56
- setting on ETEPs, 106
- setting the EncryptTight password, 62
- strong password conventions on the ETEP, 104

payload only encryption, 185

PEP

- adding, 148
- adding new PEPs and using strict authentication, 264
- configuring for EncryptTight, 55
- customized default configurations, 150
- deleting, 153
- editing, 151
- enabling the SNTP client, 149
- overview, 21
- pushing configurations, 151
- renaming, 152
- troubleshooting tools, 243–??
- viewing encryption statistics, 244
- working with large numbers of PEPs, 150

performance data, viewing, 230

ping

- pinging the management port, 227
- setting a ping tool preference, 228

PMTU configuration

- ETEP, 326

point-to-point policy

- distributed key, adding, 203
- Layer 2 example, 211
- negotiated, 335

policies

- See also* policy management with ETPM
- EncryptTight distributed key policies overview, 17
- starting ETPM, 131

ETEP

- clearing policies on the ETEP, 334
- negotiated Layer 2 point-to-point policies, 335
- setting L2 or L3 encryption, 334
- starting ETPM, 334
- traffic handling, 338

reloading, 226

policy and key information

ETEP PEPs, 244

policy constraint extension, 271

policy editor

starting ETPM, 335

Policy Enforcement Point, *see* PEP

policy management with ETPM

- allowing local site exETEPTions, 247
- conETEPTs, 181
- deleting a policy, 209
- deploying policies, 207
- editing policies, 209
- encapsulation method, 183
- encrypt all policy with exETEPTions, creating, 185

encryption algorithms, 184

encryption methods, 183

Ethernet policies, adding, 188

hub and spoke policy, adding, 191

Layer 2 Ethernet policies, overview, 138

Layer 3 IP policies, overview, 138

Layer 4 payload encryption, 185

Layer 4 policy, creating, 206

lifetime, defining, 182

mesh policy, adding, 195

minimizing policy size, 187

multicast policy, adding, 199

point to point policy, adding, 203

policy design examples, 214

policy generation and distribution, 139

policy view, 135

priority, setting, 182

rekey interval, defining, 182

scheduling rekey interval and policy lifetime refresh, 182

troubleshooting, 239, 245–248

Policy Manager

See *also* ETPM
 introduction, 20
 log file, 241
 monitoring status, 237
 port configuration See interface configuration
 port status, viewing, 232
 ports, configuring your firewall for EncrypTight, 39
 preferences
 certificate policy extensions, 270
 certificate requests, 284
 communication timeouts, 92
 importing appliance configurations, 115
 login, 63
 ping tool, 228
 policy deployment confirmation, 208
 status checking in ETEMS, 99
 status checking in ETPM, 137
 strict authentication, 93
 preserving network IP addresses, 35
 priority, for policy processing, 182
 problem and solution tables, 223
 appliance configuration, 225
 appliance unreachable, 224
 pushing configurations, 226
 software upgrades, 227
 status indicators, 226
 provisioning a new appliance
 See *also* appliance configuration
 basic procedure, 95
 importing configurations from a CSV file, 112
 working with large numbers of appliances, 111
 pushing
 configurations, 97
 software updates to appliances, 125

R

reassembling fragmented packets, ETEP, 310
 reboot
 after a software upgrade, 125
 after pushing a configuration, 151
 rebooting an appliance, 102
 rebooting an external ETKMS, 243
 refresh
 appliance status, 99
 policy lifetime, 182
 setting ETEMS status interval preferences, 99
 setting ETPM status interval preferences, 137
 reload policies
 status indicator, 226
 remote certificate authentication on the ETEP,
 328
 remote port address, 35
 remote port configuration

ETEP, 306–308
 remove element from ETPM, 134
 renaming a PEP, 152
 renew keys, scheduling, 182
 requirements
 hardware, 38
 third party software, 38
 restoring
 appliance software from a backup copy, 127
 default configuration settings, 111
 workspace, 71
 roles
 in ETEP Layer 2 policies, 337
 user roles in EncrypTight, 91
 user roles on the appliance, 91

S

SAD, exporting from the ETEP, 232
 saving
 appliance configurations, 97
 workspace, 70
 scheduling renew keys and refreshing lifetime,
 182
 Secure Hash Algorithm, 184
 security policies, See policies
 selecting appliances, 88
 service --status-all | fgrep “is running” command,
 242
 service --status-all command, 242
 session timer configuration
 EncrypTight software, 63
 SFTP server
 firewall port, 39
 third party software, 38
 using for log retrieval, 230
 using for software upgrades, 76, 126
 SHA-1, 184
 shared key example, 22
 shutdown
 external ETKMS, 243
 procedure for ETEPs, 116
 Simple Network Time Protocol
 overview, 33
 See *also* SNTP
 SNMP configuration
 ETEP, 313–316
 SNMPv3 configuration
 conETEPs, 316
 engine ID
 generating, 318
 viewing and exporting, 318
 trap host users, 319
 SNTP configuration

- editing on multiple appliances, 152
- ETEP, 329
- ETKMS, 51
- for EncrypTight PEPs, 149
- software requirements, 38
- software updates
 - appliance software
 - cancelling, 127
 - checking status, 127
 - logging upgrade status, 322
 - overview, 123
 - procedure, 125
 - for EncrypTight, 73
- SPD, exporting from the ETEP, 232
- SSH
 - troubleshooting, 225
- ssh
 - connecting to the appliance CLI, 123
 - enabling and disabling on the ETEP, 329
 - troubleshooting an ETEP connection, 225
- starting EncrypTight, 40
- statistics
 - using CLI commands to view appliance
 - statistics, 245
 - using ETEMS to view appliance statistics, 230
- status indicators
 - ETEMS, 90
 - ETPM, 135
 - troubleshooting, 240
- status refresh
 - setting the refresh interval in ETEMS, 99
 - setting the refresh interval in ETPM, 137
- status refresh, ETPM, 137
- status window, Appliances view, 98
- strict authentication
 - See also* certificates
 - about, 262
 - adding new PEPs, 264
 - communication preferences, 93
 - CRLs, 287
 - disabling, 293
 - enabling, 292
 - OCSF, 289
 - TLS with encryption and, 262
 - troubleshooting, 250
- supernetting, 161
- syslog
 - configuring for the EncrypTight application
 - log, 235
 - configuring on the ETEP, 323
 - configuring on the ETKMS, 54
 - configuring on the management PC, 43

T

- target appliances, selecting, 88
- technical support, 14
- templates
 - defining default appliance configurations, 110
- throughput
 - configuring on ETEPs, 301
 - licensed ETEP speeds, 56
- time and date properties, configuring on the
 - ETKMS, 51
- time synchronization of EncrypTight components,
 - overview, 33
- timeout values
 - EncrypTight inactivity timer, 63
 - ETEMS communication timers, 92
- TLS, 149
 - passing in the clear, ETEP, 330
 - using TLS with ETEMS, 42
- toolbars
 - Appliance Manager, 90
 - Certificate Manager, 90
 - ETEMS, 89
- Tools menu commands
 - Appliance Users, 106
 - Compare Config to Appliance, 100
 - Launch ETKMS LM, 45
 - Ping, 228
 - Put Configurations, 97
 - Reboot, 102
 - Refresh Status, 99
 - Restore From Backup, 127
 - Retrieve Appliance Logs, 228
 - Shutdown, 116
 - Ssh, 123
 - Upgrade Software, 123
- tools preferences, 227
- topologies
 - distributed key Ethernet, 138
 - distributed key IP, 138
 - negotiated Ethernet, 335
- traffic handling for Layer 2 policies
 - ETEPs, 338
- traffic statistics, 245
- transmitter behavior configuration
 - ETEP, 308
- transparent mode, 35
- transparent mode operation on the ETEP
 - enabling and disabling, 306
 - local and remote port IP addressing, 307
- Transport Layer Security (TLS), 24
 - See also* TLS
- trap configuration
 - ETEP, 315

Triple Data Encryption Standard, 184
troubleshooting
 See *also* diagnostic tools
 application log, 234
 certificate implementation errors, 249
 clearing policies on the ETEP, 334
 CLI diagnostic commands, 233
ETEMS
 appliance configuration, 225
 appliance software upgrades, 227
 appliance unreachable, 224
 pinging the management port, 227
 pushing configurations, 226
 status indicators, 226
ETKMS
 log files, 241
 rebooting, 243
 recovering the admin account, 243
 restarting an external ETKMS, 243
 server operation, 242
 shutting down an external ETKMS, 243
ETPM
 log files, 241
 monitoring status, 237
 key renewal, 240
 network connectivity problems, 248
 passing clear traffic, 246
 PEPs, 243–??
 policies, 239, 245–248
 status reporting, 240
trusted hosts
 configuring on ETEPs, 311
 troubleshooting, 224

U

uninstalling EncrypTight, 40
upgrading
 appliance software, 75, 125
 checking status, 127
 EncrypTight software, 73
user accounts
 default, 56
 EncrypTight
 adding, 66
 changing a user password, 66
 deleting, 66
 enabling user authentication, 62
 how they work with ETEP accounts, 67
 modifying, 66
 overview, 61
 ETEP
 adding an ETEP user, 106
 deleting ETEP users, 108

ETEP user roles, 102
 modifying user credentials, 108
 password enforcement policy, 103
 user name conventions, 104
 viewing users, 109

user roles
 appliance roles, 91
 EncrypTight roles, 61
 ETEP roles, 102
UTC offset, 121

V

View menu commands
 Appliance Users, 109
 Application Log, 234
 Statistics, 230
 Status, 232
views
 EncrypTight components view, 133
 ETPM editors, 134
 policy view, 135
virtual IP address
 about, 35
 for network sets, 171
 requirements, 36
virtual IP addresses, using in policies, 306
VLAN ID, 177
 adding, 177
 deleting, 179
 editing, 179
VLAN tagging, 329

W

Window menu commands
 Open, 89
workspace
 copying to a new PC, 72
 loading, 71
 restoring, 71
 saving, 70

X

XML-RPC certificate authentication on the ETEP,
 328

Black Box Tech Support: FREE! Live. 24/7.

Tech support the
way it should be.



Great tech support is just 30 seconds away at 724-746-5500 or blackbox.com.



About Black Box

Black Box Network Services is your source for more than 118,000 networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 30 seconds or less.

© Copyright 2011. All rights reserved. Black Box and the Double Diamond logo are registered trademarks of BB Technologies, Inc. Any third-party trademarks appearing in this manual are acknowledged to be the property of their respective owners.